KASPERSKY lab

Kaspersky Security Center 10

Implementierungshandbuch

Programmversion: 10 Service Pack 2, Maintenance Release 1

Sehr geehrter Benutzer!

Vielen Dank für Ihr Vertrauen. Wir hoffen, dass Ihnen dieses Dokument hilft und die meisten Fragen damit beantwortet werden können.

Erscheinungsdatum: 07.12.2016

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

Inhalt

Über dieses Dokument

Das Implementierungshandbuch für Kaspersky Security Center 10 (im Folgenden "Kaspersky Security Center") richtet sich an Experten, die für die Installation und Administration von Kaspersky Security Center zuständig sind, sowie an Experten, die für den technischen Support von Unternehmen verantwortlich sind, die Kaspersky Security Center einsetzen.

Sie können die Informationen in diesem Handbuch für die Ausführung folgender Aufgaben verwenden:

- Planung der Programminstallation (unter Berücksichtigung der Programmausführung, Systemanforderungen, typischen Schemata für Softwareverteilung und Besonderheiten der Kompatibilität mit anderen Programmen);
- Vorbereitung der Installation, Installation und Aktivierung von Kaspersky Security Center;
- Anpassung des Programms nach der Installation.

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

In diesem Abschnitt

In diesem Dokument

Das Implementierungshandbuch für Kaspersky Security Center enthält eine Einführung, Abschnitte mit der Beschreibung der Installation und der Einstellungen der Programmkomponenten, weiterhin Abschnitte mit der Beschreibung der Softwareverteilung für den Antiviren-Schutz des Netzwerks sowie Abschnitte mit den Belastungstestdaten. Dem Dokument wird darüber hinaus ein Glossar beigefügt.

Informationsquellen über das Programm (s. S. 14)

Dieser Abschnitt beschreibt die Informationsquellen für das Programm.

Je nach Dringlichkeit und Wichtigkeit Ihrer Frage können Sie die für Sie geeignete Informationsquelle auswählen.

Kaspersky Security Center (s. S. 17)

Dieser Abschnitt enthält Informationen zu Konzeption, den wichtigsten Möglichkeiten und den Programmkomponenten von Kaspersky Security Center.

Programmarchitektur (s. S. 19)

Dieser Abschnitt enthält eine Beschreibung der Komponenten von Kaspersky Security Center und deren Interaktion.

Hard- und Softwarevoraussetzungen (s. S. 20)

Dieser Abschnitt enthält Informationen zu den Software- und Hardwarevoraussetzungen für Client-Netzwerkgeräte.

Informationen zur Leistungsfähigkeit des Administrationsservers (s. S. 36)

In diesem Abschnitt sind die Ergebnisse der Leistungstests des Administrationsservers für verschiedene Hardwarekonfigurationen aufgeführt.

Typische Vorgehensweisen der Softwareverteilung (s. S. 40)

In diesem Abschnitt werden typische Vorgehensweisen der Softwareverteilung der Antiviren-Programme mithilfe von Kaspersky Security Center in einem Unternehmensnetzwerk beschrieben.

Verteilung der Antiviren-Programme in einem Unternehmen (s. S. 41)

In diesem Abschnitt werden Vorgehen zur Verteilung der Antiviren-Programme in einem Unternehmen beschrieben, die den typischen Vorgehensweisen der Softwareverteilung entsprechen.

Verteilung der Antiviren-Programme im Netzwerk eines Kundenunternehmens (s. S. 45)

In diesem Abschnitt werden Vorgehen zur Verteilung der Antiviren-Programme im Netzwerk eines Kundenunternehmens beschrieben, die den typischen Vorgehensweisen der Softwareverteilung entsprechen.

Bereitstellung des Administrationsservers (s. S. 50)

In diesem Abschnitt werden Schritte zur Bereitstellung des Administrationsservers beschrieben.

Konfiguration des Antiviren-Schutzes im Netzwerk eines Kundenunternehmens (s. S 101)

In diesem Abschnitt werden die Besonderheiten der Konfiguration des Antiviren-Schutzes über die Verwaltungskonsole im Netzwerk eines Kundenunternehmens beschrieben.

Remote-Installation von Programmen (s. S. 108)

In diesem Abschnitt werden Methoden für die Remote-Installation bzw. Deinstallation von Kaspersky Lab-Programmen auf Netzwerkgeräten beschrieben.

Lokale Installation von Programmen (s. S. 137)

In diesem Abschnitt wird der Installationsvorgang der Programme beschrieben, die nur lokal auf den Geräten installiert werden können.

Verteilung der Systeme für die Verwaltung von mobilen Geräten (s. S. 149)

In diesem Abschnitt wird die Verteilung der Verwaltungssysteme für mobile Geräte mithilfe der Protokolle Exchange ActiveSync®, iOS MDM und Kaspersky Endpoint Security beschrieben.

Verteilung von Self Service Portal (auf S. 173)

In diesem Abschnitt werden die Vorbereitung der Verteilung des Self Service Portals sowie die Schritte zur Verteilung des Self Service Portals beschrieben.

SMS-Versand in Kaspersky Security Center konfigurieren (s. S. 180)

In diesem Abschnitt wird die Installation des Tools Kaspersky SMS Broadcasting auf einem mobilen Gerät, die Synchronisierung des Tools mit dem Administrationsserver und die Konfiguration des SMS-Versandes in der Verwaltungskonsole beschrieben.

Netzwerkbelastung (s. S. 184)

Diesem Abschnitt können Informationen über den Umfang des Datenverkehrs im Netzwerk entnommen werden, mit dem zwischen den Client-Geräten und dem Administrationsserver bei wichtigen administrativen Vorgängen Daten ausgetauscht werden.

Geschwindigkeit, mit der die Datenbank des Administrationsservers mit Ereignissen gefüllt wird (s. S. 193)

In diesem Abschnitt werden Beispiele für die Geschwindigkeit aufgeführt, mit der die Datenbank des Administrationsservers mit Ereignissen gefüllt wird, die sich beim Ausführen von verwalteten Programmen ergeben.

Anfragen an den Technischen Support (s. S. 194)

Dieser Abschnitt beschreibt, wie Sie technischen Support erhalten können, und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

Glossar

In diesem Abschnitt werden die in diesem Dokument verwendeten Begriffe erläutert.

AO Kaspersky Lab (s. S. 209)

In diesem Abschnitt finden Sie Informationen zum Unternehmen Kaspersky Lab.

Informationen über den Code von Drittanbietern (s. S. 212)

Die Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich im Installationsordner des Programms befindet.

Markenrechtliche Hinweise (s. S. 213)

Dieser Abschnitt enthält Hinweise zu eingetragenen Marken.

Sachregister

Mithilfe dieses Abschnitts können Sie die gewünschten Informationen in diesem Dokument schnell finden.

Formatierung mit besonderer Bedeutung

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

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 werden in Block auf hellblauem Hintergrund unter dem Kopf "Beispiel" aufgeführt.

Textbeispiel	Beschreibung der Formatierung
Ein *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 **ENTER**-Taste. Drücken Sie die Tastenkombination **ALT**+**F4**.	Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben. Bei den durch ein Pluszeichen (+) verbundenen Tastenbezeichnungen geht es um eine Tastenkombination. Die genannten Tasten müssen gleichzeitig gedrückt werden.
Klicken Sie auf **Aktivieren**.	Die Namen von Elementen der Programmoberfläche sind halbfett geschrieben (z. B. Eingabefelder, Menüpunkte, Schaltflächen).
► *Um einen Zeitplan für die Aufgabe einzurichten, gehen Sie wie folgt vor:*	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.
Geben Sie in der Befehlszeile den Text `help` ein. Es erscheint folgende Meldung: `Geben Sie das Datum im Format TT:MM:JJ an.`	Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben: • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt • Daten, die über die Tastatur eingegeben werden müssen.
<Benutzername>	Variablen stehen in eckigen Klammern. Anstelle der Umgebungsvariablen werden entsprechende Werte gesetzt. Spitze Klammern werden dabei weggelassen.

Informationsquellen über das Programm

Dieser Abschnitt beschreibt die Informationsquellen für das Programm.

Je nach Dringlichkeit und Wichtigkeit Ihrer Frage können Sie die für Sie geeignete Informationsquelle auswählen.

In diesem Abschnitt

Quellen für die selbständige Suche nach Informationen

Sie können folgende Quellen verwenden, um nach Informationen über Kaspersky Security Center zu suchen:

- Seite von Kaspersky Security Center auf der Website von Kaspersky Lab
- Seite von Kaspersky Security Center 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 (s. Abschnitt "Technischer Support am Telefon" auf S. 194) wenden.

Um die Informationsquellen auf diesen Websites zu nutzen, ist eine Internetverbindung erforderlich.

Seite von Kaspersky Security Center auf der Website von Kaspersky Lab

Auf der Seite von Kaspersky Security Center (http://www.kaspersky.com/de/business-security/security-center) finden Sie allgemeine Informationen über das Programm, dessen Funktionen und Besonderheiten.

Die Seite von Kaspersky Security Center enthält einen Link zum Internet-Shop. In diesem Online-Shop können Sie das Programm erwerben oder das Recht für die Nutzung des Programms verlängern.

Seite von Kaspersky Security Center in der Wissensdatenbank

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

Auf der Seite von Kaspersky Security Center in der Wissensdatenbank (http://support.kaspersky.com/de/ksc10) finden Sie Artikel, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Erwerb, zur Installation und Anwendung des Programms enthalten.

Artikel der Wissensdatenbank beantworten nicht nur Fragen in Bezug auf Kaspersky Security Center, sondern auch auf andere Programme von Kaspersky Lab. Die Wissensdatenbank bietet außerdem Neuigkeiten über den Technischen Support.

Elektronisches Hilfesystem

Das Programm enthält Dateien für die vollständige und die kontextsensitive Hilfe.

Die vollständige Hilfe bietet Informationen zur Konfiguration und Verwendung von Kaspersky Security Center.

In der Kontexthilfe finden Sie Informationen zu den einzelnen Fenstern von Kaspersky Security Center, eine Beschreibung der Einstellungen von Kaspersky Security Center und Links zu den Beschreibungen der Aufgaben, in denen diese Einstellungen verwendet werden.

Die Hilfe kann als Teil des Programms aktiviert werden oder Sie können online auf der Web-Ressource von Kaspersky Lab darauf zugreifen. Wenn sich die Hilfe Online befindet, wird ein Fenster des Browsers geöffnet, wenn Sie darauf zugreifen. Für die Anzeige der Online-Hilfe ist eine Internetverbindung erforderlich.

Dokumentation

Die Programmdokumentation umfasst verschiedene Handbücher.

Das Administratorhandbuch bietet Informationen zur Konfiguration und Verwendung von Kaspersky Security Center.

Das Implementierungshandbuch bietet Informationen zu folgenden Aufgaben:

- Planung der Programminstallation (unter Berücksichtigung der Programmausführung, Systemanforderungen, typischen Schemata für Softwareverteilung und Besonderheiten der Kompatibilität mit anderen Programmen);
- Vorbereitung der Installation, Installation und Aktivierung von Kaspersky Security Center;
- Anpassung des Programms nach der Installation.

Im Handbuch "Erste Schritte" finden Sie Informationen zur raschen Nutzung des Programms (Beschreibung der Benutzeroberfläche und der wichtigsten Aufgaben, die mithilfe von Kaspersky Security Center ausgeführt werden können).

Kaspersky-Lab-Anwendungen im Forum diskutieren

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/index.php?showforum=26) diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Kommentare verfassen und neue Themen eröffnen.

Kaspersky Security Center

Dieser Abschnitt enthält Informationen zu Konzeption, den wichtigsten Möglichkeiten und den Programmkomponenten von Kaspersky Security Center.

Das Programm Kaspersky Security Center dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Das Programm ermöglicht es dem Administrator, auf detaillierte Informationen über die Sicherheitsstufe des Unternehmensnetzwerks zuzugreifen und alle Schutzkomponenten anzupassen, die auf Kaspersky-Lab-Programmen basieren.

Kaspersky Security Center ist für Administratoren von Unternehmensnetzwerken gedacht, die für die Sicherheit von Geräten in Unternehmen verantwortlich sind.

Kaspersky Security Center bietet Ihnen folgende Möglichkeiten:

- Eine Hierarchie der Administrationsserver erstellen, um das eigene Unternehmensnetzwerk sowie Netzwerke entfernter Standorte bzw. Kundenunternehmen verwalten zu können.

  Mit *Kundenunternehmen* bezeichnet man Unternehmen, deren Antiviren-Schutz von Dienstanbietern gewährleistet wird.

- Eine Hierarchie der Administrationsgruppen erstellen, um eine Gruppe von bestimmten Client-Geräten als Ganzes zu verwalten.

- Antiviren-Schutz verwalten, der auf Kaspersky-Lab-Programmen basiert.

- Images von Betriebssystemen zentral erstellen und sie auf Client-Geräten eines Netzwerks verteilen sowie die Remote-Installation von Kaspersky-Lab-Programmen und Programmen anderer Softwarehersteller durchführen.

- Kaspersky-Lab-Programme und Programme anderer Hersteller, die auf Client-Geräten installiert wurden, von einem entfernten Standort verwalten: Updates installieren, Schwachstellen suchen und schließen.

- Schlüssel für Kaspersky-Lab-Programme auf Client-Computer zentral verteilen, die Schlüsselverwendung überwachen und die Lizenzgültigkeit verlängern.

- Statistiken und Berichte über die Ausführung von Programmen und Geräten abrufen.
- Benachrichtigungen über kritische Ereignisse bei der Ausführung von Kaspersky-Lab-Programmen empfangen.
- Mobile Geräte verwalten, die Protokolle Kaspersky Security für Android ™, Exchange ActiveSync® oder iOS Mobile Device Management (iOS MDM) unterstützen.
- Verschlüsselung von Informationen, die auf Geräte-Festplatten und Wechselmedien gespeichert werden, sowie Zugriff der Benutzer auf verschlüsselte Daten verwalten.
- Inventarisierung der mit dem Unternehmensnetzwerk verbundenen Hardware durchführen.
- Dateien, die von den Schutzprogrammen in die Quarantäne oder ins Backup verschoben wurden, sowie Dateien, deren Verarbeitung durch die Schutzprogramme aufgeschoben wurde, zentral verwalten.

Programmarchitektur

Dieser Abschnitt enthält eine Beschreibung der Komponenten von Kaspersky Security Center und deren Interaktion.

Das Programm Kaspersky Security Center umfasst die folgenden Basiskomponenten:

- **Administrationsserver** (im Folgenden auch *Server*). Führt die Funktionen zum zentralen Speichern von Daten über die im Firmennetzwerk installierten Programme und deren Verwaltung aus.

- **Administrationsagent** (im Folgenden auch *Agent*). Dient der Interaktion zwischen Administrationsserver und Kaspersky-Lab-Anwendungen, die auf einem Netzwerkknoten (Arbeitsstation oder Server) installiert sind. Diese Komponente ist für alle für das System Microsoft® Windows® entwickelten Programme einheitlich.
  Für Kaspersky-Lab-Programme, die für Novell®- und Unix™-Betriebssysteme entwickelt wurden, sind eigene Versionen des Administrationsagenten vorhanden.

- **Verwaltungskonsole** (im Folgenden auch *Konsole*). Stellt die Benutzeroberfläche zu administrativen Diensten des Servers und des Agenten bereit. Die Verwaltungskonsole entspricht einer Erweiterungskomponente der Microsoft Management Console (MMC). Die Verwaltungskonsole ermöglicht das Herstellen einer Verbindung mit dem Remote-Administrationsserver über das Internet.

- **Server für mobile Geräte**. Stellt den Zugriff auf mobile Geräte bereit und ermöglicht deren Verwaltung über die Verwaltungskonsole. Der Server für mobile Geräte empfängt Informationen über mobile Geräte und speichert ihre Profile.

- **Kaspersky Security Center 10 Web Console**. Dient dazu, den Status des Antiviren-Programms im Netzwerk des Kundenunternehmens zu kontrollieren, das von Kaspersky Security Center verwaltet wird.

Hard- und Softwarevoraussetzungen

Administrationsserver

Hardwarevoraussetzungen:

- Prozessor: Taktfrequenz 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1,4 GHz.
- Arbeitsspeicher: 4 GB.
- Freier Speicherplatz auf dem Datenträger: 10 GB. Um die Funktion Systems Management verwenden zu können, müssen auf dem Laufwerk mindestens 100 GB freier Speicherplatz verfügbar sein.

Softwarevoraussetzungen:

- Microsoft® Data Access Components (MDAC) 2.8
- Windows DAC 6.0
- Microsoft Windows Installer 4.5.

Betriebssystem:

- Microsoft Windows 10 Home 32-Bit/64-Bit
- Microsoft Windows 10 Pro 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise 32-Bit/64-Bit
- Microsoft Windows 10 Education 32-Bit/64-Bit
- Microsoft Windows 10 Pro RS1 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise RS1 32-Bit/64-Bit
- Microsoft Windows 10 Education RS1 32-Bit/64-Bit

- Microsoft Windows 10 Pro RS2 32-Bit/64-Bit
- Microsoft Windows 10 Enterprise RS2 32-Bit/64-Bit
- Microsoft Windows 10 Education RS2 32-Bit/64-Bit
- Microsoft Windows 8.1 Pro 32-Bit/64-Bit
- Microsoft Windows 8.1 Enterprise 32-Bit/64-Bit
- Microsoft Windows 8 Pro 32-Bit/64-Bit
- Microsoft Windows 8 Enterprise 32-Bit/64-Bit
- Microsoft Windows 7 Professional SP1 32-Bit/64-Bit
- Microsoft Windows 7 Enterprise SP1 32-Bit/64-Bit
- Microsoft Windows 7 Ultimate SP1 32-Bit/64-Bit
- Microsoft Small Business Server 2008 Standard 64-Bit
- Microsoft Small Business Server 2008 Premium 64-Bit
- Microsoft Small Business Server 2011 Essentials 64-Bit
- Microsoft Small Business Server 2011 Premium Add-on 64-Bit
- Microsoft Small Business Server 2011 Standard 64-Bit
- Microsoft Windows Server® 2008 Datacenter SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008 Enterprise SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008 Foundation SP2 32-Bit/64-Bit
- Microsoft Windows Server 2008 SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008 Standard SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008
- Windows Server 2008 SP1

- Microsoft Windows Server 2008 R2 Server Core 64-Bit
- Microsoft Windows Server 2008 R2 Datacenter 64-Bit
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-Bit
- Microsoft Windows Server 2008 R2 Enterprise 64-Bit
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-Bit
- Microsoft Windows Server 2008 R2 Foundation 64-Bit
- Microsoft Windows Server 2008 R2 Foundation SP1 64-Bit
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-Bit
- Microsoft Windows Server 2008 R2 Standard 64-Bit
- Microsoft Windows Server 2008 R2 Standard SP1 64-Bit
- Microsoft Windows Server 2012 Server Core 64-Bit
- Microsoft Windows Server 2012 Datacenter 64-Bit
- Microsoft Windows Server 2012 Essentials 64-Bit
- Microsoft Windows Server 2012 Foundation 64-Bit
- Microsoft Windows Server 2012 Standard 64-Bit
- Microsoft Windows Server 2012 R2 Server Core 64-Bit
- Microsoft Windows Server 2012 R2 Datacenter 64-Bit
- Microsoft Windows Server 2012 R2 Essentials 64-Bit
- Microsoft Windows Server 2012 R2 Foundation 64-Bit
- Microsoft Windows Server 2012 R2 Standard 64-Bit
- Windows Storage Server 2008 R2 64-Bit
- Windows Storage Server 2012 64-Bit

- Windows Storage Server 2012 R2 64-Bit
- Windows Server 2016 Datacenter 64-Bit
- Windows Server 2016 Standard Edition 64-Bit.

Datenbankserver (kann auf einem anderen Computer installiert sein):

- Microsoft SQL Server® 2008 Express 32-Bit
- Microsoft SQL 2008 R2 Express 64-Bit
- Microsoft SQL 2012 Express 64-Bit
- Microsoft SQL 2014 Express 64-Bit
- Microsoft SQL Server 2008 (alle Versionen) 32-Bit/ 64-Bit
- Microsoft SQL Server 2008 R2 (alle Versionen) 64-Bit
- Microsoft SQL Server 2008 R2 Service Pack 2 64-Bit
- Microsoft SQL Server 2012 (alle Versionen) 64-Bit
- Microsoft SQL Server 2014 (alle Versionen) 64-Bit
- Microsoft SQL Server 2016 (alle Versionen) 64-Bit
- Microsoft Azure SQL Database
- MySQL 5.5 32-Bit/64-Bit
- MySQL Enterprise 5.5 32-Bit/64-Bit
- MySQL 5.6 32-Bit/64-Bit
- MySQL Enterprise 5.6 32-Bit/64-Bit
- MySQL 5.7 32-Bit/64-Bit
- MySQL Enterprise 5.7 32-Bit/64-Bit.

Unterstützung folgender virtuellen Plattformen:

- VMware vSphere™ 5.5
- VMware vSphere 6
- VMware™ Workstation 12.x Pro
- Microsoft Hyper-V® Server 2008
- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2008 R2 SP1
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- Microsoft Virtual PC 2007 (6.0.156.0)
- Citrix® XenServer® 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 11
- Oracle® VM VirtualBox 4.0.4-70112 (unterstützt Windows Gastbetriebssysteme).

Für die Installation des Administrationsservers auf Geräte mit dem Betriebssystem Microsoft Windows Server 2008 muss das Installationspaket "lite" verwendet werden. Vor der Installation des Administrationsservers müssen Sie die Datenbank (z. B. Microsoft SQL Server 2014) selbständig installieren.

Kaspersky Security Center 10 Web Console

Hardwarevoraussetzungen:

- Prozessor: Taktfrequenz 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1,4 GHz.
- Arbeitsspeicher: 512 MB.
- Freier Speicherplatz auf dem Datenträger: 1 GB.

Softwarevoraussetzungen:

- Für die Ausführung unter dem Betriebssysteme Microsoft Windows mit installiertem Administrationsserver von Kaspersky Security Center Version Service Pack 2:
  - Microsoft Windows 10 Home 32-Bit/64-Bit
  - Microsoft Windows 10 Pro 32-Bit/64-Bit
  - Microsoft Windows 10 Enterprise 32-Bit/64-Bit
  - Microsoft Windows 10 Education 32-Bit/64-Bit
  - Microsoft Windows 10 Pro RS1 32-Bit/64-Bit
  - Microsoft Windows 10 Enterprise RS1 32-Bit/64-Bit
  - Microsoft Windows 10 Education RS1 32-Bit/64-Bit
  - Microsoft Windows 10 Pro RS2 32-Bit/64-Bit
  - Microsoft Windows 10 Enterprise RS2 32-Bit/64-Bit
  - Microsoft Windows 10 Education RS2 32-Bit/64-Bit
  - Microsoft Windows 8.1 Pro 32-Bit/64-Bit
  - Microsoft Windows 8.1 Enterprise 32-Bit/64-Bit
  - Microsoft Windows 8 Pro 32-Bit/64-Bit
  - Microsoft Windows 8 Enterprise 32-Bit/64-Bit
  - Microsoft Windows 7 Professional SP1 32-Bit/64-Bit
  - Microsoft Windows 7 Enterprise SP1 32-Bit/64-Bit
  - Microsoft Windows 7 Ultimate SP1 32-Bit/64-Bit
  - Microsoft Small Business Server 2008 Standard 64-Bit
  - Microsoft Small Business Server 2008 Premium 64-Bit

- Microsoft Small Business Server 2011 Essentials 64-Bit
- Microsoft Small Business Server 2011 Premium Add-on 64-Bit
- Microsoft Small Business Server 2011 Standard 64-Bit
- Microsoft Windows Server® 2008 Datacenter SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008 Enterprise SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008 Foundation SP2 32-Bit/64-Bit
- Microsoft Windows Server 2008 SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008 Standard SP1 32-Bit/64-Bit
- Microsoft Windows Server 2008
- Windows Server 2008 SP1
- Microsoft Windows Server 2008 R2 Server Core 64-Bit
- Microsoft Windows Server 2008 R2 Datacenter 64-Bit
- Microsoft Windows Server 2008 R2 Datacenter SP1 64-Bit
- Microsoft Windows Server 2008 R2 Enterprise 64-Bit
- Microsoft Windows Server 2008 R2 Enterprise SP1 64-Bit
- Microsoft Windows Server 2008 R2 Foundation 64-Bit
- Microsoft Windows Server 2008 R2 Foundation SP1 64-Bit
- Microsoft Windows Server 2008 R2 SP1 Core Mode 64-Bit
- Microsoft Windows Server 2008 R2 Standard 64-Bit
- Microsoft Windows Server 2008 R2 Standard SP1 64-Bit
- Microsoft Windows Server 2012 Server Core 64-Bit
- Microsoft Windows Server 2012 Datacenter 64-Bit

- Microsoft Windows Server 2012 Essentials 64-Bit
- Microsoft Windows Server 2012 Foundation 64-Bit
- Microsoft Windows Server 2012 Standard 64-Bit
- Microsoft Windows Server 2012 R2 Server Core 64-Bit
- Microsoft Windows Server 2012 R2 Datacenter 64-Bit
- Microsoft Windows Server 2012 R2 Essentials 64-Bit
- Microsoft Windows Server 2012 R2 Foundation 64-Bit
- Microsoft Windows Server 2012 R2 Standard 64-Bit
- Windows Storage Server 2008 R2 64-Bit
- Windows Storage Server 2012 64-Bit
- Windows Storage Server 2012 R2 64-Bit
- Windows Server 2016 Datacenter 64-Bit
- Windows Server 2016 Standard Edition 64-Bit
- Debian GNU/Linux® 7.x 32-Bit
- Debian GNU/Linux 7.x 64-Bit
- Ubuntu Server 14.04 LTS 32-Bit
- Ubuntu Server 14.04 LTS 64-Bit
- CentOS 6.x (bis 6.6) 64-Bit.

Versionen von Betriebssystemen, die mit systemd arbeiten, beispielsweise Fedora® 17, werden von Kaspersky Security Center 10 Web Console nicht unterstützt.

Webserver:

- Apache 2.4.25 (für Windows) 32-Bit
- Apache 2.4.25 (für Linux) 32-Bit/64-Bit.

Für die Nutzung von Kaspersky Security Center 10 Web Console können folgende Browser verwendet werden:

- Microsoft Internet Explorer® 9 und höher
- Microsoft® Edge
- Chrome™ 53 und höher
- Firefox™ 47 und höher
- Safari® 8 unter dem Betriebssystem Mac OS X 10.10 (Yosemite)
- Safari 9 unter dem Betriebssystem Mac OS X 10.11 (El Capitan).

Server für mobile Geräte iOS Mobile Device Management (iOS MDM)

Hardwarevoraussetzungen:

- Prozessor: Taktfrequenz 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1,4 GHz.
- Arbeitsspeicher: 2 GB.
- Freier Speicherplatz auf dem Datenträger: 2 GB.

Softwarevoraussetzungen: Betriebssystem Microsoft Windows (die Version des unterstützten Betriebssystems wird durch die Anforderungen des Administrationsservers bestimmt).

Exchange ActiveSync-Server für mobile Geräte

Die Software- und Hardwareanforderungen für den Exchange ActiveSync-Server für mobile Geräte sind in vollem Umfang durch die Anforderungen für Microsoft Exchange Server gedeckt.

Kompatibel mit Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 und Microsoft Exchange Server 2013.

Verwaltungskonsole

Hardwarevoraussetzungen:

- Prozessor: Taktfrequenz 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1,4 GHz.
- Arbeitsspeicher: 512 MB.
- Freier Speicherplatz auf dem Datenträger: 1 GB.

Softwarevoraussetzungen:

- Betriebssystem: Microsoft Windows (die Version des unterstützten Betriebssystems wird durch die Anforderungen des Administrationsservers bestimmt).
- Microsoft Management Console 2.0.
- Microsoft Windows Installer 4.5.
- Unter Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 oder Microsoft Windows Vista® muss Microsoft Internet Explorer 7.0 und höher installiert sein.
- Für Microsoft Windows 7 wird Microsoft Internet Explorer 8.0 und höher benötigt.
- Für Microsoft Windows 8 und 10 wird Microsoft Internet Explorer 10.0 und höher benötigt.
- Für Microsoft Windows 10 wird Microsoft Edge benötigt.

Administrationsagent

Hardwarevoraussetzungen:

- Prozessor: Taktfrequenz 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1,4 GHz.
- Arbeitsspeicher: 512 MB.
- Freier Speicherplatz auf dem Datenträger: 1 GB.

Wenn das Gerät mit installiertem Administrationsagenten zusätzlich die Rolle des Update-Agenten erfüllt, muss dieses Gerät zusätzlich folgenden Hardwarevoraussetzungen genügen:

- Prozessor: Taktfrequenz 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1,4 GHz.
- Arbeitsspeicher: 1 GB.
- Freier Speicherplatz auf dem Datenträger: 4 GB.

Softwarevoraussetzungen:

- Windows Embedded POSReady 7 32-Bit/64-Bit
- Windows Embedded Standard 7 SP1 32-Bit/64-Bit
- Windows Embedded 8 Standard 32-Bit/64-Bit
- Windows Embedded 8 Industry Pro 32-Bit/64-Bit
- Windows Embedded 8 Industry Enterprise 32-Bit/64-Bit
- Windows Embedded 8.1 Industry Pro 32-Bit/64-Bit
- Windows Embedded 8.1 Industry Enterprise 32-Bit/64-Bit
- Windows Embedded 8.1 Industry Update 32-Bit/64-Bit
- Windows 10 Home 32-Bit/64-Bit
- Windows 10 Pro 32-Bit/64-Bit
- Windows 10 Enterprise 32-Bit/64-Bit
- Windows 10 Education 32-Bit/64-Bit
- Windows 10 Home RS1 32-Bit/64-Bit
- Windows 10 Pro RS1 32-Bit/64-Bit
- Windows 10 Enterprise RS1 32-Bit/64-Bit
- Windows 10 Education RS1 32-Bit/64-Bit
- Windows 10 Home RS2 32-Bit/64-Bit

- Windows 10 Pro RS2 32-Bit/64-Bit
- Windows 10 Enterprise RS2 32-Bit/64-Bit
- Windows 10 Education RS2 32-Bit/64-Bit
- Microsoft Windows 2000 Server
- Windows 8.1 Pro 32-Bit/64-Bit
- Windows 8.1 Enterprise 32-Bit/64-Bit
- Windows 8 Pro 32-Bit/64-Bit
- Windows 8 Enterprise 32-Bit/64-Bit
- Windows 7 Professional SP1 32-Bit/64-Bit
- Windows 7 Enterprise SP1 32-Bit/64-Bit
- Windows 7 Ultimate SP1 32-Bit/64-Bit
- Windows 7 Professional 32-Bit/64-Bit
- Windows 7 Enterprise 32-Bit/64-Bit
- Windows 7 Ultimate 32-Bit/64-Bit
- Windows 7 Home Basic 32-Bit/64-Bit
- Windows 7 Premium 32-Bit/64-Bit
- Windows Vista Business SP1 32-Bit/64-Bit
- Windows Vista Enterprise SP1 32-Bit/64-Bit
- Windows Vista Ultimate SP1 32-Bit/64-Bit
- Windows Vista Business SP2 32-Bit/64-Bit
- Windows Vista Enterprise SP2 32-Bit/64-Bit
- Windows Vista Ultimate SP2 32-Bit/64-Bit
- Windows XP Professional SP3 32-Bit

- Windows XP Professional SP2 32-Bit/64-Bit
- Windows XP Home SP3 32-Bit
- Essential Business Server 2008 64-Bit
- Small Business Server 2003 Standard SP1 32-Bit
- Small Business Server 2003 Premium SP1 32-Bit
- Small Business Server 2008 Standard 64-Bit
- Small Business Server 2008 Premium 64-Bit
- Small Business Server 2011 Essentials 64-Bit
- Small Business Server 2011 Premium Add-on 64-Bit
- Small Business Server 2011 Standard 64-Bit
- Windows Home Server 2011 64-Bit
- Windows MultiPoint™ Server 2011 64-Bit
- Windows Server 2003 Enterprise SP2 32-Bit/64-Bit
- Windows Server 2003 Standard SP2 32-Bit/64-Bit
- Windows Server 2003 R2 Enterprise SP2 32-Bit/64-Bit
- Windows Server 2003 R2 Standard SP2 32-Bit/64-Bit
- Windows Server 2008 Datacenter SP1 32-Bit/64-Bit
- Windows Server 2008 Enterprise SP1 32-Bit/64-Bit
- Windows Server 2008 Enterprise SP2 32-Bit/64-Bit
- Windows Server 2008 SP1 Server Core 32-Bit/64-Bit
- Windows Server 2008 Standard SP1 32-Bit/64-Bit
- Windows Server 2008 32-Bit/64-Bit
- Windows Server 2008 R2 Server Core 64-Bit

- Windows Server 2008 R2 Datacenter 64-Bit
- Windows Server 2008 R2 Datacenter SP1 64-Bit
- Windows Server 2008 R2 Enterprise 64-Bit
- Windows Server 2008 R2 Enterprise SP1 64-Bit
- Windows Server 2008 R2 Foundation 64-Bit
- Windows Server 2008 R2 Foundation SP1 64-Bit
- Windows Server 2008 R2 SP1 Core Mode 64-Bit
- Windows Server 2008 R2 Standard 64-Bit
- Windows Server 2008 R2 Standard SP1 64-Bit
- Windows Server 2012 Server Core 64-Bit
- Windows Server 2012 Datacenter 64-Bit
- Windows Server 2012 Essentials 64-Bit
- Windows Server 2012 Foundation 64-Bit
- Windows Server 2012 Standard 64-Bit
- Windows Server 2012 R2 Server Core 64-Bit
- Windows Server 2012 R2 Datacenter 64-Bit
- Windows Server 2012 R2 Essentials 64-Bit
- Windows Server 2012 R2 Foundation 64-Bit
- Windows Server 2012 R2 Standard 64-Bit
- Windows Server 2016 Datacenter Edition
- Windows Server 2016 Standard Edition
- Windows Nano Server 2016
- Windows Storage Server 2008 R2 64-Bit

- Windows Storage Server 2012 64-Bit
- Windows Storage Server 2012 R2 64-Bit
- Debian GNU/Linux 8.x 32-Bit
- Debian GNU/Linux 8.x 64-Bit
- Debian GNU/Linux 7.x (bis 7.8) 32-Bit
- Debian GNU/Linux 7.x (bis 7.8) 64-Bit
- Ubuntu Server 16.04 LTS x32 32-Bit
- Ubuntu Server 16.04 LTS x64 64-Bit
- Ubuntu Server 14.04 LTS x32 32-Bit
- Ubuntu Server 14.04 LTS x64 64-Bit
- Ubuntu Desktop 16.04 LTS x32 32-Bit
- Ubuntu Desktop 16.04 LTS x64 64-Bit
- Ubuntu Desktop 14.04 LTS x32 32-Bit
- Ubuntu Desktop 14.04 LTS x64 64-Bit
- CentOS 6.x (bis 6.6) 64-Bit
- CentOS 7.0 64-Bit
- Red Hat Enterprise Linux Server 7.0 64-Bit
- SUSE Linux Enterprise Server 12 64-Bit
- SUSE Linux Enterprise Desktop 12 64-Bit
- Mac OS X ®10.4 (Tiger®)
- Mac OS X 10.5 (Leopard®)
- Mac OS X 10.6 (Snow Leopard®)
- OS X 10.7 (Lion)

- OS X 10.8 (Mountain Lion)
- OS X 10.9 (Mavericks)
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS® Sierra (10.12)
- VMware vSphere™ 5.5
- VMware vSphere 6
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- Microsoft Hyper-V Server 2008
- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2008 R2 SP1
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7.

Die neuesten Informationen über die Hardware- bzw. Softwareanforderungen können Sie dem Abschnitt Systemanforderungen (http://support.kaspersky.com/de/ksc10#requirements) der Kaspersky Security Center-Seite auf der Website des Technischen Supports entnehmen.

Informationen zur Leistungsfähigkeit des Administrationsservers

In diesem Abschnitt sind die Ergebnisse der Leistungstests des Administrationsservers für verschiedene Hardwarekonfigurationen aufgeführt.

Mit den Testdaten für die Leistungsfähigkeit des Administrationsservers wurde die maximale Anzahl an Client-Geräten definiert, mit denen der Administrationsserver eine Synchronisierung in den vorgegebenen Zeiträumen ausführen kann. Diese Informationen eignen sich dafür, optimale Schemata für die Softwareverteilung des Antiviren-Schutzes in Unternehmensnetzwerken zu wählen.

Bei den Tests wurden die folgenden Hardwarekonfigurationen für den Administrationsserver verwendet:

- 32-Bit-Betriebssystem (Doppelkernprozessor Intel® Core™2 Duo E8400 mit einer Taktfrequenz von 3.00 GHz, 4 GB RAM, Festplatte SATA 500 GB)
- 64-Bit-Betriebssystem (Vierkernprozessor Intel Xeon® E5450 mit einer Taktfrequenz von 3.00 GHz, 8 GB RAM, Festplatte SAS 2x320 RAID 0).

Microsoft SQL 2005x32 Enterprise Edition wurde auf demselben Client-Gerät installiert wie der Administrationsserver.

Der Administrationsserver der beiden Hardware-Konfigurationen unterstützte das Erstellen von 200 virtuellen Administrationsservern.

Tabelle 2. Ergebnisse der zusammengefassten Belastungstests des Administrationsservers für ein 32-Bit-Betriebssystem

Synchronisierungsintervall, Min.	Anzahl der verwalteten Geräte
15	5.000
30	10.000
45	15.000
60	20.000

Tabelle 3. Ergebnisse der zusammengefassten Belastungstests des Administrationsservers für ein 64-Bit-Betriebssystem

Synchronisierungsintervall, Min.	Anzahl der verwalteten Geräte
15	10.000
30	20.000
45	30.000
60	40.000

Es wird nicht empfohlen, beim Herstellen einer Verbindung zwischen dem Administrationsserver und dem Datenbankserver MySQL und SQL Express das Programm für die Verwaltung von mehr als 5.000 Geräten zu verwenden.

Struktur des Antiviren-Schutzes im Unternehmen auswählen

Die Auswahl der Struktur des Antiviren-Schutzes im Unternehmen wird durch folgende Faktoren bestimmt:

- Netztopologie des Unternehmens
- Organisationsstruktur
- Anzahl der für den Antiviren-Schutz zuständigen Mitarbeiter und deren Aufgabenverteilung
- Hardwareressourcen, die für die Installation von Antiviren-Schutzkomponenten zur Verfügung gestellt werden können
- Bandbreite der Kommunikationskanäle, die für den Einsatz der Antiviren-Schutzkomponenten im Netzwerk des Unternehmens zur Verfügung gestellt werden können
- Annehmbare Zeit für die Durchführung von wichtigen administrativen Vorgängen im Netzwerk des Unternehmens. Zu wichtigen administrativen Vorgängen gehören zum Beispiel die Verbreitung von Updates der Antiviren-Datenbanken und die Veränderung von Richtlinien für die Client-Geräte.

Bei der Wahl der Antiviren-Schutzstruktur empfiehlt es sich, zunächst die vorhandenen Netzwerk- und Hardwareressourcen zu bestimmen, die sich für das zentrale Virenschutz-System verwenden lassen.

Für die Analyse der Netzwerk- und Hardwareinfrastruktur wird die folgende Vorgehensweise empfohlen:

1. Legen Sie die folgenden Einstellungen für das Netzwerk fest, in dem die Antiviren-Programme verteilt werden sollen:
    - Anzahl der Netzwerksegmente
    - Geschwindigkeit der Kommunikationskanäle zwischen den einzelnen Netzwerksegmenten

- Anzahl der verwalteten Geräte in jedem Netzwerksegment
- Bandbreite aller Kommunikationskanäle, die für den Antiviren-Schutz zur Verfügung gestellt werden kann.

2. Definieren Sie die zulässige Dauer für die Durchführung wichtiger administrativer Operationen für alle verwalteten Geräte.
3. Analysieren Sie die Informationen aus Punkten 1 und 2 sowie Daten aus den Belastungstests des Administrationssystems (s. Abschnitt "Netzwerkbelastung" auf S. 184). Beantworten Sie anhand der durchgeführten Analyse folgende Fragen:
   - Können alle Clients mit einem Administrationsserver bedient werden oder ist eine Hierarchie der Administrationsserver nötig?
   - Welche Hardwarekonfiguration der Administrationsserver ist nötig, um alle Clients in der in Punkt 2 festgelegten Zeit zu bedienen?
   - Ist eine Verwendung von Update-Agenten nötig, um die Belastung der Kommunikationskanäle zu verringern?

Nachdem Sie die angeführten Fragen beantwortet haben, können Sie denkbare Antiviren-Schutzstrukturen für das Unternehmen zusammenstellen.

Im Netzwerk des Unternehmens kann eine der folgenden typischen Antiviren-Schutzstrukturen verwendet werden:

- Ein einziger Administrationsserver. Alle Client-Geräte sind mit einem einzigen Administrationsserver verbunden Der Administrationsserver agiert als Update-Agent.
- Ein einziger Administrationsserver mit Update-Agenten. Alle Client-Geräte sind mit einem einzigen Administrationsserver verbunden Im Netzwerk sind Client-Geräte zur Verfügung gestellt, die als Update-Agenten agieren.
- Administrationsserver-Hierarchie. Für jedes Netzwerksegment wird ein separater Administrationsserver zur Verfügung gestellt, der in die allgemeine Hierarchie der Administrationsserver eingeschlossen ist. Der Haupt-Administrationsserver agiert als Update-Agent.
- Administrationsserver-Hierarchie mit Update-Agenten. Für jedes Netzwerksegment wird ein separater Administrationsserver zur Verfügung gestellt, der in die allgemeine Hierarchie der Administrationsserver eingeschlossen ist. Im Netzwerk sind Client-Geräte zur Verfügung gestellt, die als Update-Agenten agieren.

Typische Vorgehensweisen der Softwareverteilung

In diesem Abschnitt werden typische Vorgehensweisen der Softwareverteilung der Antiviren-Programme mithilfe von Kaspersky Security Center in einem Unternehmensnetzwerk beschrieben.

Das System muss vor unbefugten Zugriffen aller Art geschützt werden. Es wird empfohlen, vor der Installation des Programms alle verfügbaren Updates des Betriebssystems zu installieren.

Sie können Antiviren-Programme im Netzwerk eines Unternehmens mithilfe von Kaspersky Security Center verteilen, indem Sie folgende Vorgehensweisen verwenden:

- Verteilung der Antiviren-Programme über Kaspersky Security Center auf eine der folgenden Weisen:
  - über die Verwaltungskonsole;
  - über Kaspersky Security Center 10 Web Console.

  Die Installation von Kaspersky Lab-Programmen auf Client-Geräten und die Verbindung von Client-Geräten mit dem Administrationsserver erfolgt automatisch mithilfe von Kaspersky Security Center.

  Die wichtigste Vorgehensweise für Softwareverteilung ist die Verteilung des Antiviren-Schutzes über die Verwaltungskonsole. Kaspersky Security Center 10 Web Console ermöglicht die Installation von Kaspersky-Lab-Programmen über einen Webbrowser.
- Manuelle Verteilung der Antiviren-Programme mithilfe autonomer Installationspakete, die in Kaspersky Security Center erstellt wurden.

  Die Installation von Kaspersky Lab-Programmen auf den Client-Geräten und dem Administrator-Arbeitsplatz erfolgt manuell. Die Einstellungen für die Verbindung der Client-Geräte mit dem Administrationsserver werden bei der Installation des Administrationsagenten vorgegeben.

  Diese Variante der Softwareverteilung wird empfohlen, wenn keine Remote-Installation möglich ist.

Außerdem ermöglicht Kaspersky Security Center die Verteilung von Antiviren-Programmen mithilfe von Gruppenrichtlinien des Active Directory®. Weitere Details siehe: Hilfe für Kaspersky Security Center.

Softwareverteilung innerhalb eines Unternehmens

In diesem Abschnitt werden Vorgehen zur Verteilung der Antiviren-Programme in einem Unternehmen beschrieben, die den typischen Vorgehensweisen der Softwareverteilung entsprechen.

In diesem Abschnitt

Softwareverteilung über die Verwaltungskonsole innerhalb eines Unternehmens

Die Remote-Installation der erforderlichen Software wird vom Kaspersky Security Center Administrator (im Folgenden auch Administrator genannt) über die Verwaltungskonsole durchgeführt. Der Verteilungsvorgang besteht in diesem Fall aus folgenden Schritten:

1. Der Administrator stellt den Administrationsserver auf folgende Weise bereit:
    a. Installiert Kaspersky Security Center auf einem ausgewählten Gerät.
    b. Installiert die Verwaltungskonsole auf dem Administrator-Arbeitsplatz (bei Bedarf).
    c. Passt die Einstellungen des Administrationsservers an.
2. Wenn es erforderlich ist, erstellt der Administrator in Kaspersky Security Center eine Hierarchie der Administrationsserver.

3. Der Administrator erstellt eine Struktur mit Administrationsgruppen und weist die Client-Geräte des Unternehmens den Administrationsgruppen zu.
4. Der Administrator erstellt in Kaspersky Security Center Installationspakete für den Administrationsagenten und die erforderlichen Kaspersky-Lab-Programme und konfiguriert sie.
5. Der Administrator wählt in der Verwaltungskonsole Geräte aus, auf denen die gewählten Programme installiert werden sollen.
6. Der Administrator erstellt und startet die Aufgaben zur Remote-Installation der gewählten Programme über die Verwaltungskonsole.
7. Bei Bedarf führt der Administrator eine zusätzliche Konfiguration der installierten Programme über die Verwaltungskonsole (mithilfe von Richtlinien und lokalen Programmeinstellungen) durch.

Softwareverteilung mithilfe von Kaspersky Security Center 10 Web Console innerhalb eines Unternehmens

Die Remote-Installation der erforderlichen Software mittels Kaspersky Security Center 10 Web Console führt der Administrator von Kaspersky Security Center (im Folgenden auch Administrator genannt) durch. Der Verteilungsvorgang besteht in diesem Fall aus folgenden Schritten:

1. Der Administrator stellt den Administrationsserver auf folgende Weise bereit:
    a. Installiert Kaspersky Security Center auf einem ausgewählten Gerät.
    b. Installiert Kaspersky Security Center 10 Web Console auf demselben Gerät.
    c. Installiert die Verwaltungskonsole auf dem Administrator-Arbeitsplatz (bei Bedarf).
    d. Passt die Einstellungen des Administrationsservers für die Arbeit mit Kaspersky Security Center 10 Web Console an.
2. Der Administrator erstellt in Kaspersky Security Center einen virtuellen Administrationsserver zur Verwaltung der Client-Geräte.

3. Der Administrator wählt im Unternehmensnetzwerk ein Gerät aus, das die Rolle des Update-Agenten übernehmen soll, und installiert den Administrationsagenten lokal auf diesem Gerät.

   Daraufhin bestimmt Kaspersky Security Center das Gerät, auf dem der Administrationsagent installiert wurde, automatisch zum Update-Agenten und konfiguriert es bei der ersten Verbindung zum Administrationsserver als Verbindungs-Gateway.

4. Der Administrator erstellt auf dem virtuellen Administrationsserver Installationspakete für den Administrationsagenten und die erforderlichen Kaspersky-Lab-Programme und konfiguriert sie.

5. Der Administrator startet die Kaspersky Security Center 10 Web Console.

6. Der Administrator startet in der Kaspersky Security Center 10 Web Console die Installation der gewählten Programme auf den Geräten.

7. Bei Bedarf führt der Administrator eine zusätzliche Konfiguration der installierten Programme über die Verwaltungskonsole (mithilfe von Richtlinien und lokalen Programmeinstellungen) durch.

Manuelle Softwareverteilung innerhalb eines Unternehmens

Die manuelle Installation der erforderlichen Software mithilfe autonomer Installationspakete wird vom Administrator von Kaspersky Security Center durchgeführt (im Folgenden auch Administrator genannt). Der Verteilungsvorgang besteht in diesem Fall aus folgenden Schritten:

1. Der Administrator stellt den Administrationsserver auf folgende Weise bereit:

   a. Installiert Kaspersky Security Center auf einem ausgewählten Gerät.

   b. Installiert die Verwaltungskonsole auf dem Administrator-Arbeitsplatz (bei Bedarf).

   c. Passt die Einstellungen des Administrationsservers an.

2. Wenn es erforderlich ist, erstellt der Administrator in Kaspersky Security Center eine Hierarchie der Administrationsserver.

3. Der Administrator erstellt eine Struktur der Administrationsgruppen.

4. Der Administrator erstellt in Kaspersky Security Center Installationspakete für den Administrationsagenten und die erforderlichen Kaspersky-Lab-Programme und konfiguriert sie.

5. Der Administrator erstellt autonome Installationspakete für gewählte Programme.

6. Der Administrator lässt autonome Installationspakete auf die Client-Geräte übertragen (z. B. durch das Veröffentlichen eines Links auf die autonomen Pakete).

7. Die Benutzer der Client-Geräte starten die Installation von Programmen mithilfe der empfangenen autonomen Installationspakete.

8. Nach dem Verbindungsaufbau mit dem Administrationsserver werden die Client-Geräte in die Administrationsgruppen verschoben, die in den Eigenschaften der autonomen Installationspakete angegeben wurden.

Softwareverteilung im Netzwerk eines Kundenunternehmens

In diesem Abschnitt werden Vorgehen zur Verteilung der Antiviren-Programme im Netzwerk eines Kundenunternehmens beschrieben, die den typischen Vorgehensweisen der Softwareverteilung entsprechen.

In diesem Abschnitt

Softwareverteilung über die Verwaltungskonsole im Netzwerk eines Kundenunternehmens

Die Remote-Installation der erforderlichen Software wird vom Kaspersky Security Center Administrator (im Folgenden auch Administrator genannt) über die Verwaltungskonsole durchgeführt. Der Verteilungsvorgang besteht in diesem Fall aus folgenden Schritten:

1. Der Administrator von Kaspersky Security Center stellt den Administrationsserver auf folgende Weise bereit:
    a. Installiert Kaspersky Security Center auf einem ausgewählten Gerät.
    b. Installiert Kaspersky Security Center 10 Web Console auf demselben Gerät.
    c. Installiert die Verwaltungskonsole auf dem Administrator-Arbeitsplatz (bei Bedarf).
    d. Passt die Einstellungen des Administrationsservers für die Arbeit mit Kaspersky Security Center 10 Web Console an.

2. Der Administrator von Kaspersky Security Center erstellt in Kaspersky Security Center einen virtuellen Administrationsserver zur Verwaltung von Client-Geräten des Kundenunternehmens.

3. Der Administrator von Kaspersky Security Center wählt im Unternehmensnetzwerk ein Gerät aus, das die Rolle des Update-Agenten übernehmen soll, und installiert lokal auf diesem Gerät den Administrationsagenten.

   Daraufhin bestimmt Kaspersky Security Center das Client-Gerät, auf dem der Administrationsagent installiert wurde, automatisch zum Update-Agenten und konfiguriert es bei der ersten Verbindung zum Administrationsserver als Verbindungs-Gateway.

4. Der Administrator von Kaspersky Security Center erstellt auf dem virtuellen Administrationsserver Installationspakete für den Administrationsagenten und die erforderlichen Kaspersky-Lab-Programme und konfiguriert sie.

5. Der Administrator von Kaspersky Security Center wählt in der Verwaltungskonsole Geräte aus, auf welchen die gewählten Programme installiert werden sollen.

6. Der Administrator erstellt und startet die Aufgaben zur Remote-Installation der gewählten Programme über die Verwaltungskonsole.

7. Bei Bedarf führt der Administrator eine zusätzliche Konfiguration der installierten Programme über die Verwaltungskonsole (mithilfe von Richtlinien und lokalen Programmeinstellungen) durch.

Softwareverteilung mithilfe der Kaspersky Security Center 10 Web Console im Netzwerk eines Kundenunternehmens

Die Remote-Installation der erforderlichen Software mittels Kaspersky Security Center 10 Web Console führt der Administrator von Kaspersky Security Center zusammen mit dem Administrator des Kundenunternehmens durch. Der Verteilungsvorgang besteht in diesem Fall aus folgenden Schritten:

1. Der Administrator von Kaspersky Security Center stellt den Administrationsserver auf folgende Weise bereit:

    a. Installiert Kaspersky Security Center auf einem ausgewählten Gerät.

    b. Installiert Kaspersky Security Center 10 Web Console auf demselben Gerät.

    c. Installiert die Verwaltungskonsole auf dem Administrator-Arbeitsplatz (bei Bedarf).

    d. Passt die Einstellungen des Administrationsservers für die Arbeit mit Kaspersky Security Center 10 Web Console an.

2. Der Administrator von Kaspersky Security Center erstellt in Kaspersky Security Center einen virtuellen Administrationsserver zur Verwaltung von Client-Geräten des Kundenunternehmens.

3. Der Administrator des Kundenunternehmens wählt im Unternehmensnetzwerk ein Gerät aus, das die Rolle des Update-Agenten übernehmen soll, und installiert lokal auf diesem Geräte den Administrationsagenten.

    Daraufhin bestimmt Kaspersky Security Center das Client-Gerät, auf dem der Administrationsagent installiert wurde, automatisch zum Update-Agenten und konfiguriert es bei der ersten Verbindung zum Administrationsserver als Verbindungs-Gateway.

4. Der Administrator von Kaspersky Security Center erstellt auf dem virtuellen Administrationsserver Installationspakete für den Administrationsagenten und die erforderlichen Kaspersky-Lab-Programme und konfiguriert sie.

5. Der Administrator des Kundenunternehmens startet in Kaspersky Security Center 10 Web Console die Installation der gewählten Programme auf den Client-Geräten.

6. Bei Bedarf führt der Administrator von Kaspersky Security Center eine zusätzliche Konfiguration der installierten Programme über die Verwaltungskonsole (mithilfe von Richtlinien und lokalen Programmeinstellungen) durch.

Manuelle Softwareverteilung im Netzwerk eines Kundenunternehmens

Die manuelle Installation der erforderlichen Software mithilfe der autonomen Installationspakete wird vom Administrator von Kaspersky Security Center zusammen mit dem Administrator des Kundenunternehmens durchgeführt. Der Verteilungsvorgang besteht in diesem Fall aus folgenden Schritten:

1. Der Administrator von Kaspersky Security Center stellt den Administrationsserver auf folgende Weise bereit:

    a. Installiert Kaspersky Security Center auf einem ausgewählten Gerät.

    b. Installiert Kaspersky Security Center 10 Web Console auf demselben Gerät.

    c. Installiert die Verwaltungskonsole auf dem Administrator-Arbeitsplatz (bei Bedarf).

    d. Passt die Einstellungen des Administrationsservers für die Arbeit mit Kaspersky Security Center 10 Web Console an.

2. Der Administrator von Kaspersky Security Center erstellt in Kaspersky Security Center einen virtuellen Administrationsserver zur Verwaltung von Client-Geräten des Kundenunternehmens.

3. Der Administrator des Kundenunternehmens wählt im Unternehmensnetzwerk ein Gerät aus, das die Rolle des Update-Agenten übernehmen soll, und installiert lokal auf diesem Geräte den Administrationsagenten.

   Daraufhin bestimmt Kaspersky Security Center das Client-Gerät, auf dem der Administrationsagent installiert wurde, automatisch zum Update-Agenten und konfiguriert es bei der ersten Verbindung zum Administrationsserver als Verbindungs-Gateway.

4. Der Administrator von Kaspersky Security Center erstellt auf dem virtuellen Administrationsserver Installationspakete für den Administrationsagenten und die erforderlichen Kaspersky-Lab-Programme und konfiguriert sie.

5. Der Administrator von Kaspersky Security Center erstellt autonome Installationspakete für die gewählten Programme.

6. Der Administrator von Kaspersky Security Center leitet ein autonomes Installationspaket an das Kundenunternehmen weiter (z.B. durch die Veröffentlichung des Links auf das autonome Installationspaket in Kaspersky Security Center 10 Web Console).

7. Der Administrator des Kundenunternehmens leitet das autonome Installationspaket über Kaspersky Security Center 10 Web Console auf die ausgewählten Geräte weiter.

8. Benutzer der Client-Geräte starten die Installation des Programms mithilfe des heruntergeladenen autonomen Installationspakets.

9. Nach dem Verbindungsaufbau mit dem Administrationsserver werden die Client-Geräte in die Administrationsgruppe verschoben, die in den Eigenschaften des autonomen Installationspakets angegeben wurde.

Bereitstellung des Administrationsservers

In diesem Abschnitt werden Schritte zur Bereitstellung des Administrationsservers beschrieben.

Die Schritte für die Softwareverteilung werden für zwei Varianten der Arbeit mit dem Programm beschrieben:

- Bereitstellung des Administrationsservers in einem Unternehmen;
- Bereitstellung des Administrationsservers für den Schutz eines Kundenunternehmens.

> Wenn es erforderlich ist, den Administrationsserver in einem Unternehmen bereitzustellen, das entfernte Standorte umfasst, die nicht zum Unternehmensnetzwerk gehören, können Sie sich an die Reihenfolge der Softwareverteilung für Dienstanbieter halten.

Kaspersky Security Center kann in die Plattform von Microsoft Network Access Protection (NAP) integriert werden. Dadurch wird die Steuerung des Zugriffs von Client-Geräten auf das Netzwerk ermöglicht. Um die Funktionstüchtigkeit des Betriebssystems bei gleichzeitigem Einsatz des Programms Kaspersky Security Center und Microsoft NAP zu überprüfen, muss zusätzlich die Komponente System Health Validator installiert werden (s. Abschnitt "Kaspersky Security Center SHV installieren und konfigurieren" auf S. 89).

Im Folgenden werden im Abschnitt Aktionen beschrieben, die zu den aufgeführten Schritten der Softwareverteilung gehören.

In diesem Abschnitt

Schritte für die Bereitstellung des Administrationsservers in einem Unternehmen

► *Gehen Sie wie folgt vor, um den Administrationsserver in einem Unternehmen bereitzustellen:*

1. Installieren Sie Kaspersky Security Center auf dem Administrator-Arbeitsplatz.

2. Passen Sie die Einstellungen des Administrationsservers an.

Schritte für die Bereitstellung des Administrationsservers für den Antiviren-Schutz eines Kundenunternehmens

► *Gehen Sie wie folgt vor, um den Administrationsserver zum Antiviren-Schutz im Netzwerk eines Kundenunternehmens bereitzustellen:*

1. Installieren Sie Kaspersky Security Center auf dem Administrator-Arbeitsplatz.
2. Installieren Sie die Kaspersky Security Center 10 Web Console auf dem Administrator-Arbeitsplatz.
3. Passen Sie die Einstellungen des Administrationsservers für die Arbeit mit Kaspersky Security Center 10 Web Console an.

Update der vorherigen Version von Kaspersky Security Center

Sie können den Administrationsserver 10 auf dem Gerät installieren, auf dem die vorherige Version des Administrationsservers installiert ist. Beim Update auf die Version 10 bleiben Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Vor dem Update von Kaspersky Security Center müssen verschlüsselte Laufwerke des Geräts, auf denen Programmkomponenten (Administrationsserver, Administrationsagenten) installiert sind, entschlüsselt werden. Nach dem Update von Kaspersky Security Center können die zuvor entschlüsselten Laufwerke erneut verschlüsselt werden.

► *Um den Administrationsserver 9.0 auf die Version 10 zu aktualisieren, gehen Sie wie folgt vor:*

1. Starten Sie die ausführbare Datei setup.exe für die Version 10.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

   Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** starten Sie den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

2. Lesen Sie sorgfältig den Endbenutzer-Lizenzvertrag, den Sie mit Kaspersky Lab abschließen. Wenn Sie mit allen Punkten der Vereinbarung einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**.

   Die Programminstallation wird fortgesetzt. Der Installationsassistent schlägt Ihnen vor, eine Backup-Kopie der Daten auf dem Administrationsserver für Kaspersky Security Center 9.0 zu erstellen.

   Kaspersky Security Center unterstützt die Wiederherstellung von Daten aus einer Backup-Kopie der Daten des Administrationsservers, die mit einer älteren Programmversion angelegt wurde.

3. Wenn Sie eine Sicherheitskopie im geöffneten Fenster **Sicherungskopie des Administrationsservers erstellen** erstellen möchten, aktivieren Sie das Kontrollkästchen **Sicherungskopie des Administrationsservers erstellen**.

   Eine Backup-Kopie der Daten des Administrationsservers wird mithilfe des Tools klbackup erstellt. Das Tool gehört zum Programmpaket und wird im Stammverzeichnis der Installation von Kaspersky Security Center abgelegt.

   > Detaillierte Informationen über das Tool Verschieben ins Backup und Wiederherstellung von Daten finden Sie im Abschnitt "Anhang" des Administratorhandbuchs für Kaspersky Security Center.

4. Installieren Sie den Administrationsserver für Version 10. Folgen Sie dazu den Anweisungen des Installationsassistenten.

Es wird nicht empfohlen, die Ausführung des Installationsassistenten abzubrechen. Das Abbrechen des Update-Vorgangs während der Installation des Administrationsservers kann zur Funktionsunfähigkeit von Kaspersky Security Center 9.0 führen.

5. Erstellen und starten Sie für Geräte, auf denen der Administrationsagent einer vorherigen Version installiert wurde, die Aufgabe zur Remote-Installation einer neuen Version des Administrationsagenten (s. Abschnitt "Programme mithilfe der Aufgabe zur Remote-Installation installieren" auf S. 111).

   Nach der Durchführung der Aufgabe zur Remote-Installation wird die Version des Administrationsagenten aktualisiert.

Sollten bei der Installation des Administrationsservers Probleme auftreten, können Sie die vorherige Version des Administrationsservers wiederherstellen, indem Sie die vor dem Update erstellte Backup-Kopie der Serverdaten heranziehen.

Wenn im Netzwerk mindestens ein Administrationsserver der neuen Version installiert ist, besteht die Möglichkeit, die anderen Administrationsserver im Netzwerk mithilfe der Aufgabe zur Remote-Installation zu installieren, in welcher das Installationspaket des Administrationsservers verwendet wird.

Kaspersky Security Center installieren und deinstallieren

In diesem Abschnitt wird die lokale Installation der Anwendungskomponenten von Kaspersky Security Center beschrieben. Es sind zwei Installationsarten verfügbar:

- **Standard**. In diesem Fall wird ein minimaler Satz der Programmkomponenten installiert. Diese Installationsart empfiehlt sich für Netzwerke mit bis zu 200 Geräten.
- **Benutzerdefiniert**. In diesem Fall können Sie einzelne Komponenten für die Installation auswählen und zusätzliche Programmeinstellungen anpassen. Diese Installationsart empfiehlt sich für Netzwerke mit mehr als 200 Geräten. Die benutzerdefinierte Installation eignet sich für erfahrene Benutzer.

Wenn im Netzwerk mindestens ein Administrationsserver installiert ist, können die Server auf den anderen Geräten des Netzwerks mit der Aufgabe zur Remote-Installation durch Erzwungene Installation installiert werden (s. Abschnitt "Installation von Programmen mit der Aufgabe zur Remote-Installation" auf S. 111). Verwenden Sie beim Erstellen der Aufgabe zur Remote-Installation das Installationspaket des Administrationsservers.

In diesem Abschnitt

Vorbereitung der Installation

Vor der Installation müssen Sie sich vergewissern, dass die Hard- und Softwarevoraussetzungen des Geräts den Anforderungen des Administrationsservers und der Verwaltungskonsole entsprechen.

Kaspersky Security Center speichert Daten in der Datenbank des SQL-Servers. Dafür wird zusammen mit Kaspersky Security Center standardmäßig Microsoft SQL Server 2014 Express SP1 installiert. Zur Speicherung von Informationen können auch andere SQL-Server verwendet werden. In diesem Fall müssen sie im Netzwerk vor der Installation von Kaspersky Security Center installiert sein.

Zur Installation von Kaspersky Security Center werden die Rechte des lokalen Administrators auf dem Gerät verwendet, auf dem die Installation ausgeführt werden soll.

Damit nach der Installation die Programmkomponenten richtig funktionieren, müssen auf dem Gerät alle nötigen Ports geöffnet sein (s. Tabelle unten).

Tabelle 4. Ports, die von Kaspersky Security Center verwendet werden

Port	Protokoll.	Beschreibung
Geräte, auf dem der Administrationsserver installiert ist		
8060	HTTP	Wird für die Verbindung mit dem Webserver für den Einsatz von Kaspersky Security Center 10 Web Console und die Organisation des innerbetrieblichen Portals verwendet.
8061	HTTPS	Wird für die Verbindung mit dem Webserver für den Einsatz von Kaspersky Security Center 10 Web Console und die Organisation des innerbetrieblichen Portals verwendet. Beim Verbindungsaufbau wird eine Verschlüsselung verwendet.
13000	TCP	Werden zu folgenden Zwecken verwendet: • Empfang der Daten von Client-Geräten; • Verbindung mit den Update-Agenten; • Verbindung mit untergeordneten Administrationsservern. Es wird dabei eine geschützte SSL-Verbindung hergestellt.
13000	UDP	Übertragung der Daten über ausgeschaltete Geräte.
13111	TCP	Wird für die Verbindung mit dem Proxy-Server KSN verwendet.
13291	TCP	Wird für die Verbindung der Verwaltungskonsole mit dem Administrationsserver verwendet. Es wird dabei eine geschützte SSL-Verbindung hergestellt.
13292	TCP	Verbindung mit mobilen Geräten.

Port	Protokoll.	Beschreibung
14000	TCP	Werden zu folgenden Zwecken verwendet: • Empfang der Daten von Client-Geräten; • Verbindung mit den Update-Agenten; • Verbindung mit untergeordneten Administrationsservern. Es wird dabei keine geschützte SSL-Verbindung hergestellt.
17000	TCP	Wird für die Verbindung mit dem Aktivierungs-Proxyserver verwendet Es wird dabei eine geschützte SSL-Verbindung hergestellt.
17100	TCP	Wird für den Verbindungsaufbau zum Aktivierungs-Proxyserver für die Aktivierung von mobilen Geräten verwendet.
Gerät, das vom Update-Agenten benannt wurde		
13000	TCP	Verbindung von Client-Geräten mit dem Update-Agenten.
13001	TCP	Verbindung von Client-Geräten mit dem Update-Agenten, wenn der Update-Agent ein Gerät mit installiertem Administrationsserver ist.
14000	TCP	Verbindung von Client-Geräten mit dem Update-Agenten.
14001	TCP	Verbindung von Client-Geräten mit dem Update-Agenten, wenn der Update-Agent ein Gerät mit installiertem Administrationsserver ist.
Client-Geräte mit installiertem Administrationsagenten		
7	UDP	Verwendung der Funktionen von Wake On Lan.
9	UDP	
67	UDP	Wird bei der Bereitstellung von Betriebssystemabbildern auf dem Gerät verwendet, der als PXE-Server festgelegt ist.
69	UDP	

Port	Protokoll.	Beschreibung
15000	UDP	Empfang von Verbindungsanfragen mit dem Administrationsserver, sodass Gerätedaten in Echtzeit eintreffen.
15001	UDP	Interaktion mit dem Update-Agenten.

Bei ausgehenden Verbindungen der Client-Geräte zum Administrationsserver und den Update-Agenten wird der Port-Bereich 1024–5000 (TCP-Protokoll) verwendet. Unter Microsoft Windows Vista und Microsoft Windows Server 2008 liegt der ausgehende Port-Bereich standardmäßig bei 49152–65535 (TCP-Protokoll).

Standardinstallation

► *Um die Standardinstallation von Kaspersky Security Center auf einem lokalen Gerät durchzuführen, gehen Sie wie folgt vor:*

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

   Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** starten Sie den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

2. Lesen Sie sorgfältig den Endbenutzer-Lizenzvertrag, den Sie mit Kaspersky Lab abschließen. Wenn Sie mit allen Punkten der Vereinbarung einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**. Die Programminstallation wird fortgesetzt.

   Außerdem kann der Installationsassistent Ihnen vorschlagen, die Lizenzverträge für die im Programmpaket von Kaspersky Security Center verfügbaren Verwaltungs-Plug-ins für Programme zu beachten und die Bedingungen dieser Endbenutzer-Lizenzverträge zu akzeptieren.

3. Wählen Sie den Installationstyp **Standard** aus, und klicken Sie auf **Weiter**.

Daraufhin extrahiert der Assistent die Dateien aus dem Lieferumfang und schreibt sie auf die Festplatte des Geräts.

Im letzten Fenster des Assistenten wird Ihnen vorgeschlagen, die Verwaltungskonsole zu starten. Beim ersten Start der Konsole können Sie eine Erstkonfiguration des Programms ausführen (weitere Details siehe: *Kaspersky Security Center Administratorhandbuch*).

Nach Abschluss des Installationsassistenten werden die folgenden Programmkomponenten auf der Festplatte installiert, auf welcher das Betriebssystem installiert wurde:

- Administrationsserver (zusammen mit Serverversion des Administrationsagenten);
- Verwaltungskonsole;
- Alle im Programmpaket verfügbaren Verwaltungs-Plug-ins für Programme.

Außerdem werden die folgenden Programme installiert, wenn sie zuvor nicht installiert wurden:

- Microsoft Windows Installer 4.5
- Microsoft .NET Framework 2.0 SP2
- Microsoft SQL Server® 2008 R2 Express Edition SP2.

Benutzerdefinierte Installation

► *Um eine benutzerdefinierte Installation von Kaspersky Security Center auf einem lokalen Gerät vorzunehmen,*

starten Sie die ausführbare Datei setup.exe.

Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können. Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center Administrationsserver installieren** starten Sie den Installationsassistenten des Administrationsservers. Folgen Sie den Anweisungen des Assistenten.

Im Folgenden werden die Schritte des Installationsassistenten für das Programm sowie die Aktionen beschrieben, die Sie in jedem Schritt ausführen können.

Schritte des Assistenten

Schritt 1. Lizenzvertrag anzeigen

Machen Sie sich in diesem Schritt des Installationsassistenten mit dem Lizenzvertrag vertraut, den Sie mit Kaspersky Lab abschließen.

Außerdem werden Sie eventuell aufgefordert, sich mit den Lizenzverträgen für die im Programmpaket von Kaspersky Security Center verfügbaren Verwaltungs-Plug-ins für Programme vertraut zu machen.

Lesen Sie den Endbenutzer-Lizenzvertrag sorgfältig durch. Wenn Sie mit allen Punkten der Vereinbarung einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**. Die Installation des Programms auf Ihrem Gerät wird fortgesetzt.

Falls Sie dem Lizenzvertrag nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

Schritt 2. Installationsart auswählen

Geben Sie die Installationsart **Benutzerdefiniert** an.

Schritt 3. Anwendungskomponenten für die Installation a uswählen

Wählen Sie die Komponenten des Administrationsservers von Kaspersky Security Center aus, die installiert werden sollen:

- **Unterstützung für mobile Geräte**. Diese Komponente ermöglicht die Verwaltung des Schutzes für mobile Geräte über Kaspersky Security Center.
- **SNMP-Agent**. Empfängt statistische Daten für den Administrationsserver mit dem SNMP-Protokoll. Die Komponente steht zur Verfügung, wenn bei der Installation des Programms auf dem Gerät die SNMP-Komponente installiert ist.

  > Nach der Installation von Kaspersky Security Center befinden sich die für den Empfang von Statistikdaten benötigten mib-Dateien im Installationsverzeichnis im Unterordner SNMP.

Im Dialogfenster des Assistenten werden Hilfeinformationen über die ausgewählte Komponente und den für die Installation der Komponente benötigten Speicherplatz angezeigt.

Die Komponenten Administrationsagent und Verwaltungskonsole werden in der Liste der Komponenten nicht angezeigt. Diese Komponenten werden automatisch installiert und deren Installation kann nicht abgebrochen werden.

Mit der Komponente Administrationsserver wird die Serverversion des Administrationsagenten auf dem Gerät installiert. Dessen gemeinsame Installation mit der üblichen Version des Administrationsagenten ist nicht möglich. Wenn bereits eine Serverversion des Administrationsagenten auf Ihrem Gerät installiert ist, deinstallieren Sie diese und starten Sie die Installation des Administrationsservers erneut.

Geben Sie in diesem Schritt des Assistenten auch den Ordner für die Installation der Komponenten des Administrationsservers an. Standardmäßig werden die Komponenten in den Ordner <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center installiert. Wenn kein Ordner mit diesem Namen vorhanden ist, wird er automatisch während des Installationsvorgangs angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** wechseln.

Schritt 4. Netzwerkgröße auswählen

Geben Sie die Größe des Netzwerks an, in dem Kaspersky Security Center installiert wird. In Abhängigkeit von der Anzahl an Geräten im Netzwerk passt der Assistent die Installationseinstellungen und die Darstellung der Programmoberfläche an.

In der Tabelle unten sind die Installationseinstellungen für das Programm und die Darstellung der Programmoberfläche bei Auswahl von verschiedenen Netzwerkgrößen aufgeführt.

Tabelle 5. Installationseinstellungen je nach Netzwerkgröße

Einstellungen	1–100 Geräte	100-1000 Geräte	1000-5000 Geräte	Mehr als 5000 Geräte
Anzeige des Knotens der untergeordneten und virtuellen Administrationsserver in der Konsolenstruktur und aller Einstellungen, die für untergeordnete und virtuelle Server relevant sind	nicht vorhanden	nicht vorhanden	vorhanden	vorhanden
Anzeige der Abschnitte **Sicherheit** im Eigenschaftenfenster des Administrationsservers und der Administrationsgruppen	nicht vorhanden	nicht vorhanden	vorhanden	vorhanden
Zufällige Verteilung der Startzeit für die Update-Aufgabe auf Client-Geräten	nicht vorhanden	im Intervall 5 Minuten	im Intervall 10 Minuten	im Intervall 10 Minuten

Es wird nicht empfohlen, beim Herstellen einer Verbindung zwischen dem Administrationsserver und dem Datenbankserver MySQL und SQL Express das Programm für die Verwaltung von mehr als 5000 Geräten zu verwenden.

Schritt 5. Benutzerkonto auswählen

Wählen Sie ein Benutzerkonto aus, unter dem der Administrationsserver als Dienst auf diesem Gerät gestartet werden soll:

- **System-Benutzerkonto**. Der Administrationsserver wird unter dem Benutzerkonto und mit den Rechten für das *System-Benutzerkonto* gestartet.

  Damit Kaspersky Security Center fehlerfrei funktioniert, muss das Benutzerkonto für den Start des Administrationsservers über Administratorrechte für das Speichern der Administrationsserver-Datenbank verfügen.

  Unter Microsoft Windows Vista und neueren Microsoft Windows-Betriebssystemen kann der Administrationsserver nicht mit dem System-Benutzerkonto installiert werden. In diesen Fällen steht die Variante **Automatisch erstelltes Benutzerkonto (<Kontoname>)** zur Verfügung.

- **Benutzerkonto**: Der Administrationsserver wird unter dem Benutzerkonto des angegebenen Benutzers gestartet. In diesem Fall initiiert der Administrationsserver alle Vorgänge mit den Rechten dieses Benutzerkontos. Geben Sie mit der Schaltfläche **Auswählen** einen Benutzer an, dessen Benutzerkonto verwendet wird, und legen Sie ein Kennwort fest.

Bei Verwendung des SQL-Servers muss bei der Benutzerkonto-Authentifizierung von Microsoft Windows dem Benutzerkonto Zugriff auf die Datenbank gewährt werden. Das Benutzerkonto muss dem Besitzer der Datenbank von Kaspersky Anti-Virus zugewiesen sein. Standardmäßig ist das Schema dbo zu verwenden.

Wenn Sie später das Benutzerkonto des Administrationsservers austauschen wollen, können Sie das Tool Wechsel des Benutzerkontos für den Administrationsserver (*klsrvswch*) verwenden. Detaillierte Informationen hierzu finden Sie im *Administratorhandbuch für Kaspersky Security Center*.

Schritt 6. Benutzerkonto für den Start der Dienste konfigurieren

Wählen Sie das Benutzerkonto, unter dem die Dienste von Kaspersky Security Center auf diesem Gerät gestartet werden sollen:

- **Automatisch erstelltes Konto**. Kaspersky Security Center erstellt ein Benutzerkonto in der Gruppe KLAdmins. Die Dienste von Kaspersky Security Center werden unter dem erstellten Benutzerkonto gestartet.
- **Benutzerkonto festlegen**. Die Dienste von Kaspersky Security Center werden unter dem angegebenen Benutzerkonto eines Benutzers gestartet. Geben Sie mithilfe der Schaltfläche **Auswählen** das Benutzerkonto an und geben Sie das Kennwort ein.

Schritt 7. Datenbank auswählen

Wählen Sie in diesem Schritt des Installationsassistenten die Ressource Microsoft SQL Server (SQL Express) oder MySQL, die zum Speichern der Datenbank des Administrationsservers dienen soll.

> Wenn Sie Kaspersky Security Center auf dem Server installieren, der die Rolle des Domänencontrollers ohne Schreibberechtigung (RODC) übernimmt, ist die Installation von Microsoft SQL Server (SQL Express) nicht vorgesehen. In diesem Fall wird empfohlen, die MySQL-Ressource zu verwenden, um Kaspersky Security Center fehlerfrei zu installieren.

Eine Beschreibung für die Datenbankstruktur des Administrationsservers finden Sie in der Datei klakdb.chm, die sich im Installationsordner von Kaspersky Security Center befindet.

Schritt 8. Einstellungen des SQL-Servers konfigurieren

In diesem Schritt des Installationsassistenten erfolgt die Konfiguration des SQL-Servers.

In Abhängigkeit davon, welche Datenbank ausgewählt wurde, sind folgende Varianten für die Konfiguration des SQL-Servers verfügbar:

- Wenn Sie im vorherigen Schritt SQL Express oder Microsoft SQL Server ausgewählt haben, wählen Sie eine der folgenden Varianten:

  - Wenn im Unternehmensnetzwerk ein SQL-Server installiert wurde, geben Sie im Feld **Name des SQL-Servers** seinen Namen ein.

    Im Feld **Name des SQL-Servers** ist standardmäßig der Name des SQL-Servers angegeben, der auf dem Gerät erkannt wurde, von dem aus Kaspersky Security Center installiert werden soll. Mit der Schaltfläche **Durchsuchen** kann die Liste aller im Netzwerk installierten SQL-Server angezeigt werden.

    > Wenn der Administrationsserver unter dem Benutzerkonto des lokalen Administrators oder unter dem System-Benutzerkonto aufgerufen wird, ist die Schaltfläche **Durchsuchen** nicht verfügbar.

    Geben Sie in das Feld **Name der Datenbank** den Namen der Datenbank an, die zum Speichern der Daten vom Administrationsserver dienen soll. Standardmäßig wird die Datenbank unter dem Namen **KAV** angelegt.

    > Wenn geplant ist, mithilfe von Kaspersky Security Center weniger als 5000 Geräte zu verwalten, kann Microsoft SQL Express 2005/2008 verwendet werden.
    > Wenn die voraussichtliche Anzahl der Geräte, die mit Kaspersky Security Center verwaltet werden sollen, über 5000 liegt, wird die Verwendung von Microsoft SQL 2005/2008 empfohlen.

Es wird empfohlen, eine andere SQL Server Edition als Express zu verwenden, wenn die Komponente Aktivitätskontrolle für Programme für die Verwaltung von mehr als 50 Geräten verwendet werden soll.

- Wenn im Unternehmensnetzwerk kein SQL-Server installiert ist, wählen Sie die Variante **Microsoft SQL Server 2014 Express SP1 installieren** aus.

  Der Installationsassistent für das Programm installiert Microsoft SQL Server 2014 Express SP1. Die nötigen Einstellungen werden automatisch eingerichtet.

- Wenn im vorangegangenen Schritt MySQL-Server ausgewählt wurde, geben Sie im Feld **Name des SQL-Servers** dessen Namen (standardmäßig wird die IP-Adresse des Geräts verwendet, auf dem Kaspersky Security Center installiert werden soll) und im Feld **Port** den Port für die Verbindung (standardmäßig wird Port 3306 verwendet) ein.

  Geben Sie im Feld **Name der Datenbank** den Namen der Datenbank ein, die zum Speichern der Daten des Administrationsservers erstellt wird (standardmäßig wird die Datenbank unter dem Namen **KAV** erstellt).

Wenn Sie einen SQL-Server auf demselben Gerät manuell installieren wollen, von dem aus die Installation von Kaspersky Security Center erfolgt, müssen Sie die Installation abbrechen und sie nach der Installation des SQL-Servers erneut starten. Die unterstützten SQL-Server werden in den Systemanforderungen aufgezählt.

Wenn Sie einen SQL-Server auf einem Remote-Gerät manuell installieren wollen, muss der Installationsassistent für Kaspersky Security Center nicht abgebrochen werden. Installieren Sie den SQL-Server, und kehren Sie zur Installation von Kaspersky Security Center zurück.

Schritt 9. Authentifizierungsmodus auswählen

Definieren Sie den Modus der Authentifizierung, der beim Verbindungsaufbau des Administrationsservers mit dem SQL-Server herangezogen werden soll.

In Abhängigkeit von der ausgewählten Datenbank können Sie folgende Authentifizierungsmodi auswählen:

- Wählen Sie für SQL Express oder Microsoft SQL Server eine der folgenden Varianten aus:
  - **Microsoft Windows Authentifizierungsmodus**: In diesem Fall wird beim Überprüfen der Berechtigungen das Benutzerkonto für den Start des Administrationsservers herangezogen.
  - **SQL-Server Authentifizierungsmodus**: Bei dieser Variante wird für die Überprüfung der Berechtigungen das im Fenster angegebene Benutzerkonto herangezogen. Nehmen Sie Eingaben in die Felder **Benutzerkonto**, **Kennwort** und **Kennwort bestätigen** vor.

  Wenn sich die Datenbank des Administrationsservers auf einem anderen Gerät befindet und das Benutzerkonto des Administrationsservers keinen Zugriff auf den Datenbankserver hat, muss bei der Installation oder dem Update des Administrationsservers die Authentifizierung des SQL-Servers verwendet werden. Dieser Fall kann eintreten, wenn sich das Gerät mit der Datenbank nicht in der Domäne befindet oder der Administrationsserver unter dem Benutzerkonto Lokales System installiert wurde.
- Geben Sie für den MySQL-Server ein Benutzerkonto und ein Kennwort an.

Schritt 10. Gemeinsamen Ordner festlegen

Definieren Sie den Speicherort und den Namen des gemeinsamen Ordners, der für folgende Zwecke verwendet wird:

- Die Speicherung der Dateien, die für die Remote-Installation von Programmen benötigt werden (die Dateien werden beim Erstellen der Installationspakete auf den Administrationsserver kopiert)
- Die Speicherung der Updates, die aus den Update-Quellen auf den Administrationsserver kopiert werden.

Allen Benutzern wird für diese Ressource die allgemeine Leseberechtigung erteilt.

Sie können eine der folgenden beiden Varianten auswählen:

- **Freigegebenen Ordner erstellen**: Neuen Ordner erstellen. Geben Sie den Pfad zum Ordner im Feld unten an.
- **Vorhandenen freigegebenen Ordner auswählen**: Gemeinsamen Ordner aus den bereits vorhandenen Ordnern auswählen.

Der Ordner darf sich lokal auf dem Rechner befinden, von dem die Installation erfolgt, oder auf einem Remote-Gerät. Dabei handelt es sich um ein beliebiges Client-Gerät, das zum Netzwerk des Unternehmens gehört. Sie können einen gemeinsamen Ordner durch Klicken auf die Schaltfläche **Durchsuchen** oder manuell angeben, indem Sie den UNC-Pfad in das entsprechende Feld eingeben (Beispiel: \\server\Share).

Standardmäßig wird der lokale Ordner Share in dem Ordner angelegt, der für die Installation der Programmkomponenten von Kaspersky Security Center angegeben wurde.

Schritt 11. Verbindungseinstellungen mit Administrationsserver konfigurieren

Passen Sie die Einstellungen für die Verbindung mit dem Administrationsserver an:

- **Port**. Portnummer für das Herstellen einer Verbindung mit dem Administrationsserver. Standardmäßig wird Port 14000 verwendet.
- **SSL-Port**. Portnummer für das Herstellen einer sicheren Verbindung mit dem Administrationsserver über das SSL-Protokoll. Standardmäßig wird Port 13000 verwendet.

Wenn der Administrationsserver mit dem Betriebssystem Microsoft Windows XP Service Pack 2 ausgeführt wird, blockiert die integrierte Firewall die TCP-Ports mit den Adressen 13000 und 14000. Damit auf das Gerät zugegriffen werden kann, auf dem der Administrationsserver ausgeführt wird, müssen diese Ports manuell geöffnet werden.

Schritt 12. Adresse des Administrationsservers eingeben

Legen Sie die Adresse des Administrationsservers fest. Sie können eine der folgenden Varianten auswählen:

- **Name der DNS-Domäne**. Diese Variante wird dann eingesetzt, wenn im Netzwerk ein DNS-Server existiert, den die Client-Geräte verwenden, um die Adresse des Administrationsservers zu beziehen.
- **NetBIOS-Name**. Diese Variante wird eingesetzt, wenn die Client-Geräte die Adresse des Administrationsservers mit dem NetBIOS-Protokoll beziehen oder im Netzwerk ein WINS-Server vorhanden ist.
- **IP-Adresse**. Diese Variante wird eingesetzt, wenn der Administrationsserver eine statische IP-Adresse aufweist, die sich zu keinem Zeitpunkt ändert.

Schritt 13. Einstellungen für mobile Geräte konfigurieren

Dieser Schritt des Installationsassistenten ist verfügbar, wenn Sie für die Installation die Komponente **Unterstützung für mobile Geräte** ausgewählt haben.

Geben Sie zum Abschließen mobiler Geräte den Namen des Administrationsservers an.

Schritt 14. Verwaltungs-Plug-ins für Programme wählen

Wählen Sie die Verwaltungs-Plug-ins für Kaspersky-Lab-Programme, die gemeinsam mit Kaspersky Security Center installiert werden sollen.

Schritt 15. Entpacken und Installation der Dateien auf der Festplatte

Nach der Konfiguration der Installationseinstellungen für die Komponenten von Kaspersky Security Center können Sie die Installation auf der Festplatte starten.

Wenn zusätzliche Programme für den Start der Installation erforderlich sind, meldet dies der Installationsassistent vor der Installation von Kaspersky Security Center im Fenster **Installation der Pflichtkomponenten**. Die erforderlichen Programme werden automatisch nach dem Klicken auf die Schaltfläche **Weiter** installiert.

Installation im Silent-Modus

Kaspersky Security Center kann im Silent-Modus installiert werden, d. h. ohne die interaktive Eingabe von Installationseinstellungen.

► *Um Kaspersky Security Center im Silent-Modus auf einem lokalen Gerät zu installieren,*

geben Sie folgenden Befehl ein:

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 <setup_parameters>"
```

, wobei `setup_parameters` – Liste mit Einstellungen und Einstellungswerten, die durch Leerzeichen getrennt werden (`PRO1=PROP1VAL PROP2=PROP2VAL`). Die Datei setup.exe, die sich auf der CD-ROM des Programms Kaspersky Security Center im Ordner Server befindet.

Die Namen und die möglichen Einstellungswerte, die bei der Installation des Administrationsservers im Silent-Modus zulässig sind, werden in folgender Tabelle angegeben.

Tabelle 6. Einstellungen für die Installation des Administrationsservers im Silent-Modus

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags	• 1 – Die Bedingungen des Lizenzvertrags werden akzeptiert. • Anderer Wert oder keine Angabe – die Bedingungen des Endbenutzer-Lizenzvertrags werden abgelehnt (die Installation wird nicht ausgeführt).
INSTALLATIONMODETYPE	Installationstyp für den Administrationsserver	• Standard – standardmäßige Installation. • Custom – benutzerdefinierte Installation.
INSTALLDIR	Pfad des Installationsordners für den Administrationsserver	Zeichenfolgenwert.
ADDLOCAL	Liste der zur Installation vorgesehenen Komponenten (durch Komma getrennt) des Administrationsservers	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 Liste der Komponenten, die als Mindestvoraussetzungen für eine korrekte Installation des Administrationsservers gelten: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
NETRANGETYPE	Größe des Netzwerks (Anzahl der Geräte im Netzwerk)	• NRT_1_100 – von 1 bis 100 Geräte. • NRT_100_1000 – von 100 bis 1000 Geräte. • NRT_GREATER_1000 – Mehr als 1000 Geräte.
SRV_ACCOUNT_TYPE	Methode zum Erstellen eines Benutzerkontos, unter dem der Administrations-server als Dienst gestartet wird.	• SrvAccountDefault – Das Benutzerkonto wird automatisch erstellt. • SrvAccountUser – Das Benutzerkonto wird manuell erstellt. In diesem Fall müssen Werte für die Parameter SERVERACCOUNTNAME und SERVERACCOUNTPWD angegeben werden.
SERVERACCOUNTNAME	Benutzerkonto-Name, unter dem der Administrations-server als Dienst gestartet wird. Der Parameterwert wird angegeben, wenn SRV_ACCOUNT_TYPE=SrvAccountUser.	Zeichenfolgenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
SERVERACCOUNTPWD	Kennwort des Benutzerkontos, unter dem der Administrations-server als Dienst gestartet wird. Der Parameterwert wird angegeben, wenn SRV_ACCOUNT_TYPE=SrvAccountUser.	Zeichenfolgenwert.
SERVERCER	Die Lange des Schlüssels für das Zertifikat des Administrations-servers (in Bits).	• 1 – die Lange des Schlüssels für das Zertifikat des Administrationsservers ist 2048 Bits. • Kein Wert angegeben – die Länge des Schlüssels für das Zertifikat des Administrationsservers beträgt 1.024 Bit.
DBTYPE	Typ der Datenbank, die zum Speichern der Informations-datenbank des Administrations-servers verwendet wird.	• MySQL – MySQL-Datenbank verwenden. In diesem Fall müssen Werte für die Parameter MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME und MYSQLACCOUNTPWD angegeben werden. • MSSQL – Datenbank des Typs Microsoft SQL Server (SQL Express) verwenden. In diesem Fall müssen Werte für die Parameter MSSQLCONNECTIONTYPE und MSSQLAUTHTYPE angegeben werden.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
MYSQLSERVERNAME	Vollständiger Name des SQL-Servers. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MYSQLSERVERPORT	Portnummer für die Verbindung zum SQL-Server. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MYSQLDBNAME	Name der Datenbank, die erstellt wird, um Informationen des Administrations-servers zu speichern. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
MYSQLACCOUNTNAME	Benutzerkonto-Name für die Verbindung zur Datenbank. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MYSQLACCOUNTPWD	Kennwort des Benutzerkontos für die Verbindung zur Datenbank. Der Parameterwert wird angegeben, wenn DBTYPE=MySQL.	Zeichenfolgenwert.
MSSQLCONNECTIONTYPE	Nutzungsweise für die MSSQL-Datenbank. Der Parameterwert wird angegeben, wenn DBTYPE=MSSQL.	• InstallMSSEE – Microsoft SQL Server 2014 Express SP1 installieren. Die erforderlichen Einstellungen werden automatisch angepasst. • ChooseExisting – SQL-Server verwenden, der im Unternehmensnetzwerk installiert ist. In diesem Fall müssen Werte für die Parameter MSSQLSERVERNAME und MSSQLDBNAME angegeben werden.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
MSSQLSERVERNAME	Vollständiger Name des SQL-Servers. Der Parameterwert wird angegeben, wenn MSSQLCONNECTIONTYPE=ChooseExisting.	Zeichenfolgenwert.
MSSQLDBNAME	Name der Datenbank. Der Parameterwert wird angegeben, wenn MSSQLCONNECTIONTYPE=ChooseExisting.	Zeichenfolgenwert.
MSSQLAUTHTYPE	Autorisierungstyp für eine Verbindung mit dem SQL-Server. Der Wert der Einstellung wird angegeben, wenn DBTYPE=MSSQL.	• Windows – Authentifizierungsmodus Microsoft Windows. • SQLServer – Authentifizierungsmodus für den SQL-Server. In diesem Fall müssen Werte für die Parameter MSSQLACCOUNTNAME und MSSQLACCOUNTPWD angegeben werden.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
MSSQLACCOUNTNAME	Benutzerkonto-Name für die Verbindung zum SQL-Server. Der Parameterwert wird angegeben, wenn MSSQLAUTHTYPE=SQLServer.	Zeichenfolgenwert.
MSSQLACCOUNTPWD	Kennwort des Benutzer-kontos für die Verbindung zum SQL-Server. Der Parameterwert wird angegeben, wenn MSSQLAUTHTYPE=SQLServer.	Zeichenfolgenwert.
CREATE_SHARE_TYPE	Methode zum Erstellen eines gemeinsamen Ordners.	• Create – Gemeinsamen Ordner erstellen. In diesem Fall müssen Werte für die Parameter SHARELOCALPATH und SHAREFOLDERNAME angegeben werden. • ChooseExisting – Vorhandenen Ordner auswählen. In diesem Fall müssen Werte für den Parameter EXISTSHAREFOLDERNAME angegeben werden.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
SHARELOCALPATH	Vollständiger Pfad eines lokalen Ordners. Der Parameterwert wird angegeben, wenn CREATE_SHARE_TYPE=Create.	Zeichenfolgenwert.
SHAREFOLDERNAME	Netzwerkname des gemeinsamen Ordners. Der Parameterwert wird angegeben, wenn CREATE_SHARE_TYPE=Create.	Zeichenfolgenwert.
EXISTSHAREFOLDERNAME	Vollständiger Name eines vorhandenen gemeinsamen Ordners. Der Parameterwert wird angegeben, wenn CREATE_SHARE_TYPE=ChooseExisting.	Zeichenfolgenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
SERVERPORT	Portnummer für das Herstellen einer Verbindung mit dem Administrations-server.	Zahlenwert.
SERVERSSLPORT	Portnummer für das Herstellen einer sicheren Verbindung mit dem Administrations-server über das SSL-Protokoll.	Zahlenwert.
SERVERADDRESS	Adresse des Administrations-servers.	Zeichenfolgenwert.
MOBILESERVERADDRESS	Adresse des Administrations-servers für die Verbindung mit mobilen Geräten.	Zeichenfolgenwert.

Ausführliche Angaben über die Einstellungen für die Installation des Administrationsservers finden Sie im Abschnitt "**Benutzerdefinierte Installation**" (auf S. 59).

Änderungen am System nach der Installation

Nach der Installation der Verwaltungskonsole erscheint auf Ihrem Gerät im Menü **Start** → **Programme** → **Kaspersky Security Center** das Symbol für den Start.

Der Administrationsserver und der Administrationsagent werden auf dem Gerät als Dienste mit den Attributen installiert, die in der unten stehenden Tabelle aufgeführt sind. In der Tabelle werden auch Attribute anderer Dienste angezeigt, die auf dem Gerät nach der Installation des Administrationsservers ausgeführt werden.

Tabelle 7. Dienstattribute

Komponente	Name des Dienstes	Dargestellter Name des Dienstes	Starttyp	Benutzer-konto
Administrations-server	kladminserver	Kaspersky Security Center Administrations-server	Automatisch beim Start des Betriebs-systems	Ein vom Benutzer angegebenes oder ein speziell bei der Installation erstelltes Benutzer-konto der Art KL-AK-*
Administrations-agent	klnagent	Kaspersky Security Center Administrations-agent	Automatisch beim Start des Betriebs-systems	Lokales System

Web-Server für die Web-Konsole und die Organisation des inner-betrieblichen Portals	klwebsrv	Web-Server von Kaspersky Lab	Automatisch beim Start des Betriebs-systems	Spezielles nicht privilegiertes Benutzerkonto der Art KlScSvc-*
Aktivierungs-Proxy-Server	klactprx	Aktivierungs-Proxy-Server von Kaspersky Lab	Automatisch beim Start des Betriebssystems	Spezielles nicht privilegiertes Benutzer-konto der Art KlScSvc-*
Web-Autorisierungs-portal der Zugangs-berechtigung	klnsacwsrv	Autorisierungsportal von Kaspersky Lab	Manuell	Lokales System
Proxy-Server KSN	ksnproxy	Proxy-Server Kaspersky Security Network	Manuell	Spezielles nicht privilegiertes Benutzer-konto der Art KlScSvc-*
iOS MDM-Server	KLIOSMdmServiceSrv2	iOS MDM Mobile Devices Server	Automatisch beim Start des Betriebs-systems	Network Service
COM+-Objekt für die Interaktion mit einem	KasperskyMdmService	Kaspersky MDM for Exchange	Automatisch beim Zugriff auf ein Objekt	Benutzer-konto, das zur

Exchange-Server				Gruppe Domain User und KLMDM Role Group (KLMDM Secure Group) gehört.

Zusammen mit dem Administrationsserver wird auf dem Gerät die Serverversion des Administrationsagenten installiert. Sie gehört zum Administrationsserver, wird mit ihm installiert oder deinstalliert und kann nur mit dem lokal installierten Administrationsserver zusammenarbeiten. Sie brauchen die Einstellungen der Verbindung des Administrationsagenten mit dem Administrationsserver nicht anzupassen. Die Einstellung wird programmgesteuert unter Berücksichtigung der Tatsache, dass die Komponenten auf einem Gerät installiert sind, ausgeführt. Außerdem lassen sich diese Einstellungen in den lokalen Einstellungen des Administrationsagenten auf diesem Gerät nicht bearbeiten. Eine derartige Konfiguration verhindert zusätzliche Einstellungen und mögliche Konflikte der Komponenten bei ihrer Einzelinstallation.

Die Serverversion des Administrationsagenten wird mit den gleichen Attributen installiert und erfüllt die gleichen Programmverwaltungsfunktionen wie der standardmäßige Administrationsagent. Für diese Version gilt die Richtlinie der Administrationsgruppe, zu welcher das Client-Gerät des Administrationsservers gehört. Für die Serverversion des Administrationsagenten werden alle Aufgaben erstellt, die für den Administrationsagenten vorgesehen sind (ausgenommen Aufgabe zum Wechsel des Servers).

> Der Administrationsagent muss auf dem Gerät des Administrationsservers nicht separat installiert werden. Seine Funktion übernimmt die Serverversion des Administrationsagenten.

Sie können die Eigenschaften der Dienste des Servers, des Administrationsagenten und des Richtlinienservers von Kaspersky Lab anzeigen und deren Ausführung mithilfe der standardmäßigen Administrationsmitteln von Microsoft Windows Computerverwaltung\Dienste verfolgen. Die Verlaufsdaten für den Dienst des Administrationsservers werden im Systemprotokoll von Microsoft Windows auf dem Gerät

gespeichert, auf dem der Administrationsserver installiert ist, und zwar in einem separaten Eintrag mit dem Namen Kaspersky Event Log.

Auf dem Gerät, auf dem der Administrationsserver installiert ist, werden außerdem automatisch die Gruppen KLAdmins und KLOperators als lokale Benutzer angelegt.
Wenn der Administrationsserver unter dem Konto des Benutzers gestartet wird, der zu Domäne gehört, werden die Benutzergruppen KLAdmins und KLOperators zur Liste der Gruppen von Domänenbenutzern hinzugefügt. Die Struktur der Benutzergruppen wird mit den standardmäßigen Administrationsmitteln von Microsoft Windows geändert.

Um die E-Mail-Benachrichtigungen anzupassen, kann es erforderlich sein, dass der Administrator auf einem Mail-Server für die ESMTP-Authentifizierung ein Benutzerkonto einrichtet.

Programmdeinstallation

Sie können Kaspersky Security Center mit den Standardmitteln zur Installation und Deinstallation von Microsoft Windows-Programmen deinstallieren. Zur Deinstallation des Programms wird der Assistent gestartet, durch den alle Programmkomponenten (mit Plug-ins) vom Gerät deinstalliert werden. Wenn Sie in dem Assistenten nicht angegeben haben, dass der gemeinsame Ordner (Share) deinstalliert werden soll, können Sie ihn nach Abschluss aller deinstallationsrelevanten Aufgaben manuell deinstallieren.

Der Deinstallationsassistent für das Programm schlägt Ihnen vor, eine Backup-Kopie der Daten des Administrationsservers zu speichern.

Bei der Deinstallation von Anwendungen von Computern mit dem Betriebssystem Microsoft Windows 7 oder Microsoft Windows 2008 ist der vorzeitige Abschluss des Deinstallationsprogramms möglich. Um dies zu verhindern, deaktivieren Sie im Betriebssystem die Benutzerkontensteuerung (UAC) und starten die Deinstallation des Programms erneut.

Verwaltungskonsole auf dem Administrator-Arbeitsplatz installieren

Sie können die Verwaltungskonsole separat auf dem Administrator-Arbeitsplatz installieren und über diese Konsole den Administrationsserver verwalten.

► *Um die Verwaltungskonsole auf dem Administrator-Arbeitsplatz zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

   Starten Sie im Fenster mit der Programmauswahl über den Link **Verwaltungskonsole für Kaspersky Security Center installieren** den Installationsassistenten der Administrationskonsole. Folgen Sie den Anweisungen des Assistenten.

   > Der Installationsvorgang der Verwaltungskonsole von dem über das Internet heruntergeladenen Programmpaket stimmt mit dem Installationsvorgang der Verwaltungskonsole von CD-ROM überein.

2. Wählen Sie den Zielordner aus. Standardmäßig handelt es sich um <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center Console. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** wechseln.

3. Klicken Sie im letzten Fenster des Installationsassistenten auf die Schaltfläche **Beginnen**, um mit der Installation der Verwaltungskonsole zu beginnen.

Nach Abschluss des Assistenten wird die Verwaltungskonsole im Administrator-Arbeitsplatz installiert.

Nach Abschluss der Installation der Verwaltungskonsole muss eine Verbindung mit dem Administrationsserver hergestellt werden. Starten Sie dazu die Verwaltungskonsole und geben Sie im folgenden Fenster den Namen oder die IP-Adresse des Geräts,

auf dem der Administrationsserver installiert ist, sowie die Benutzerkonto-Einstellungen für den Verbindungsaufbau an. Nachdem die Verbindung zum Administrationsserver hergestellt wurde, können Sie den Antiviren-Schutz über diese Verwaltungskonsole verwalten.

Sie können die Verwaltungskonsole mit den Standardmitteln zur Installation und Deinstallation von Microsoft Windows-Programmen deinstallieren.

Verbindung der Verwaltungskonsole mit dem Administrationsserver anpassen

In den Vorgängerversionen von Kaspersky Security Center wurde die Verwaltungskonsole mit dem Administrationsserver über den SSL-Port TCP 13291, sowie den SSL-Port TCP 13000 verbunden. Ab der Version Kaspersky Security Center 10 Service Pack 2 sind die vom Programm verwendeten SSL-Ports streng getrennt und eine nicht bestimmungsgemäße Nutzung der Ports ist nicht möglich:

- Der SSL-Port TCP 13291 kann nur von der Verwaltungskonsole und den Automatisierungsobjekts des Tools klakaut verwendet werden.
- Der SSL-Port TCP 13000 kann nur vom Administrationsagenten, dem untergeordneten Server und dem Hauptadministrationsserver, der sich in der demilitarisieren Zone befindet, verwendet werden.

Der Port TCP 14000 kann für die Verbindung der Verwaltungskonsole, der Update-Agenten, der untergeordneten Administrationsserver und der Automatisierungsobjekte des Tools klakaut, sowie für das Abrufen der Daten von den Client-Geräten verwendet werden.

In einigen Fällen kann eine Verbindung der Verwaltungskonsole über den SSL-Port 13000 erforderlich sein:

- Wenn ein und derselbe SSL-Port sowohl für die Verwaltungskonsole als auch für andere Aktivitäten (zum Abrufen der Daten von den Client-Geräten, zur Verbindung der Update-Agenten, Verbindung der untergeordneten Administrationsserver) bevorzugt verwendet wird,

- Wenn das Automatisierungsobjekt des Tools klakaut nicht direkt mit dem Administrationsserver, sondern über den Update-Agenten in der entmilitarisierten Zone verbunden wird.

► *Um eine Verbindung der Verwaltungskonsole über den Port 13000 zu erlauben, gehen Sie wie folgt vor:*

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsserver installiert ist, z. B. lokal mit dem Befehl regedit im Menü **Start** → **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   - Für 64-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Für den Schlüssel LP_ConsoleMustUsePort13291 (DWORD) ist der Wert 00000000 festgelegt.

   Standardmäßig wird für diesen Schlüssel der Wert 1 festgelegt.

4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin kann die Verwaltungskonsole mit dem Administrationsserver über den Port 13000 eine Verbindung herstellen.

Kaspersky Security Center SHV installieren und konfigurieren

Kaspersky Security Center kann in die Plattform von Microsoft Network Access Protection (NAP) integriert werden. Microsoft NAP ermöglicht die Steuerung des Zugriffs von Client-Geräten auf das Netzwerk. Microsoft NAP geht davon aus, dass im Netzwerk ein Server verfügbar ist, auf dem das Betriebssystem Microsoft Windows Server 2008 installiert ist und der Dienst PVS (Posture Validation Server) läuft, und dass auf den Client-Geräten eines der folgenden NAP-kompatiblen Betriebssysteme ausgeführt wird: Microsoft Windows Vista, Microsoft Windows XP mit Service Pack 3 oder Microsoft Windows 7.

Bei der Interaktion von Kaspersky Security Center mit Microsoft NAP wird die Funktionstüchtigkeit des Betriebssystems von System Health Validator (im Folgenden Kaspersky Security Center SHV) überprüft.

► *Um Kaspersky Security Center SHV lokal auf einem Gerät zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

   Starten Sie im Fenster mit der Programmauswahl über den Link **Kaspersky Security Center SHV installieren** den Installationsassistenten für Kaspersky Security Center SHV. Folgen Sie den Anweisungen des Assistenten.

   > Der Installationsvorgang von Kaspersky Security Center SHV von dem aus dem Internet heruntergeladenen Programmpaket stimmt mit dem Installationsvorgang von CD-ROM überein.

2. Legen Sie den Zielordner fest. Standardmäßig handelt es sich um <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center SHV. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** wechseln.

3. Klicken Sie im letzten Fenster des Installationsassistenten auf die Schaltfläche **Beginnen**, um mit der Installation von Kaspersky Security Center SHV zu beginnen.

Nach Abschluss des Assistenten wird Kaspersky Security Center SHV auf Ihrem Gerät installiert.

Sie können Kaspersky Security Center SHV mit den Standardmitteln zur Installation und Deinstallation von Microsoft Windows-Programmen deinstallieren. Daraufhin wird der Assistent gestartet, durch den alle Anwendungskomponenten vom Gerät deinstalliert werden.

Installation der Kaspersky Security Center 10 Web Console

Auf dem Gerät, auf dem Kaspersky Security Center 10 Web Console installiert werden soll, muss die Verwaltungskonsole installiert sein (s. Abschnitt "Verwaltungskonsole auf dem Administrator-Arbeitsplatz installieren" auf S. 86).

> Auf Geräten mit den Betriebssystemen Windows 7, Windows Server 2008 und Windows Vista muss der Patch KB2533623 (https://support.microsoft.com/de-de/kb/2533623) installiert sein.

Für die Installation von Kaspersky Security Center 10 Web Console sind die Rechte eines lokalen Administrators erforderlich.

► *Um Kaspersky Security Center 10 Web Console auf einem lokalen Gerät zu installieren,*

starten Sie die Datei install.exe auf der CD-ROM des Programms Kaspersky Security Center 10 Web Console.

Die Installation wird von einem Assistenten begleitet. Der Installationsassistent schlägt Ihnen vor, die Installationseinstellungen anzupassen. Folgen Sie den Anweisungen.

> Der Installationsvorgang von Kaspersky Security Center 10 Web Console von dem aus dem Internet heruntergeladenen Programmpaket stimmt mit dem Installationsvorgang von CD-ROM überein.

Schritte des Assistenten

Schritt 1. Lizenzvertrag anzeigen

Machen Sie sich in diesem Schritt des Installationsassistenten mit dem Lizenzvertrag vertraut, den Sie mit Kaspersky Lab abschließen.

Lesen Sie den Endbenutzer-Lizenzvertrag sorgfältig durch. Wenn Sie mit allen Punkten der Vereinbarung einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**. Die Installation des Programms auf Ihrem Gerät wird fortgesetzt.

Falls Sie dem Lizenzvertrag nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

> Die Remote-Installation der Kaspersky Security Center 10 Web Console mithilfe eines Installationspakets oder die lokale Installation im Silent-Modus setzt das automatische Einverständnis mit den Bedingungen des Lizenzvertrags für das zu installierende Programm voraus. Der Endbenutzer-Lizenzvertrag für ein konkretes Programm ist im Lieferumfang des entsprechenden Programms enthalten oder kann auf der Support-Seite von Kaspersky Lab eingesehen werden.

Schritt 2. Verbindung zu Kaspersky Security Center aufbauen

Wählen Sie eine Methode für die Verbindung von Kaspersky Security Center 10 Web Console mit Kaspersky Security Center aus. Es sind folgende Methoden verfügbar:

- **Auf einem lokalen Gerät installierten Apache-Server verwenden**: Bei Auswahl dieser Option erfolgt die Verbindung zwischen Kaspersky Security Center 10 Web Console und Kaspersky Security Center über einen Apache-Server, der auf dem Client-Gerät installiert wurde. (Die Installation eines Apache-Servers können Sie im nächsten Schritt des Assistenten auswählen.)

- **Auf einem Remote-Gerät installierten Apache-Server verwenden**: Sie können diese Variante auswählen, wenn ein Apache-Server auf dem Remote-Gerät mit der Linux-Plattform bereits installiert wurde. In diesem Fall wird nur der Serverteil von Kaspersky Security Center 10 Web Console lokal installiert. Um eine Verbindung zwischen Kaspersky Security Center 10 Web Console und Kaspersky Security Center herzustellen, installieren Sie auf dem Remote-Gerät den Client-Teil von Kaspersky Security Center 10 Web Console. Bei der Auswahl dieser Variante wechselt der Installationsassistent zum Schritt 8 (s. Abschnitt "Schritt 8. Installation der Kaspersky Security Center 10 Web Console starten" auf S. 95).

► *Um den Client-Teil der Kaspersky Security Center 10 Web Console auf einem Remote-Gerät unter Linux zu installieren,*

starten Sie je nach Systemtyp eine der folgenden Dateien:

- Für 32-Bit-Systeme:
  - kscwebconsole-10.<Versionsnummer>.i386.rpm
  - kscwebconsole_10.<Versionsnummer>_i386.deb.
- Für 64-Bit-Systeme:
  - kscwebconsole-10.<Versionsnummer>.x86_64.rpm
  - kscwebconsole_10.<Versionsnummer>_x86_64.deb.

Schritt 3. Zielordner auswählen

Legen Sie den Zielordner für die Installation von Kaspersky Security Center 10 Web Console fest. Standardmäßig ist es der Ordner <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center Web Console. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch erstellt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** wechseln.

Schritt 4. Installationsart für den Apache-Server auswählen

Wenn auf dem Gerät kein Apache-Server installiert ist, wird Ihnen in diesem Schritt des Installationsassistenten vorgeschlagen, den Apache HTTP-Server 2.4.25 zu installieren.

Standardmäßig ist die Installationsart Apache HTTP Server 2.4.25 aktiviert. Wenn Sie den Apache-Server nicht mithilfe des Installationsassistenten von Kaspersky Security Center 10 Web Console installieren wollen, deaktivieren Sie das Kontrollkästchen **Apache HTTP Server 2.4.25 installieren**.

Während der Installation des Apache-Servers kann ein Neustart des Geräts erforderlich sein.

Schritt 5. Apache-Server installieren

In diesem Schritt des Assistenten wird der Apache HTTP Server 2.4.25 installiert und konfiguriert.

Vor Installationsbeginn legen Sie das Zertifikat fest, das für die Verschlüsselung der Verbindung des Apache-Servers mit dem Browser des Benutzers verwendet wird. Wählen Sie eine der folgenden Varianten aus:

- **Neues Zertifikat erstellen**. Ein Zertifikat für die Arbeit über das HTTPS-Protokoll erstellen.
- **Vorhandenes auswählen**. Ein vorhandenes Zertifikat für die Arbeit über das HTTPS-Protokoll verwenden. Legen Sie das Zertifikat auf eine der folgenden Weisen fest:

- **Zertifikatsdatei auswählen**. Sie können ein vorhandenes Zertifikat auswählen, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

- **Private Schlüsseldatei auswählen**: Sie können das Zertifikat mit seiner privaten Schlüsseldatei festlegen, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

Schritt 6. Ports auswählen

Passen Sie die folgenden Einstellungen an:

- SSL-Portnummer für die geschützte Verbindung des Geräts mit dem Administrationsserver. Standardmäßig wird Port 13291 verwendet.

- Portnummer für die Verbindung des Geräts mit dem Apache-Server. Standardmäßig wird Port 9000 verwendet.

- Adresse des Geräts, auf dem der Administrationsserver installiert ist.
  In der Standardeinstellung ist die Adresse localhost festgelegt.

  Wenn sich das Gerät, auf das Kaspersky Security Center 10 Web Console installiert wird und Self Service Portal, in einer entmilitarisierten Zone befindet, aktivieren Sie das Kontrollkästchen **Verbindungs-Gateway** und geben Sie im Feld **Serveradresse** die Adresse des Verbindungs-Gateways an.

- Portnummer für die Verbindung des Geräts mit Kaspersky Security Center 10 Web Console. Standardmäßig wird Port 8080 verwendet.

- Portnummer für die Verbindung des Geräts mit dem Self Service Portal. Standardmäßig wird Port 8081 verwendet.

Nach der Installation von Kaspersky Security Center 10 Web Console und Self Service Portal können Sie die standardmäßig festgelegten Portnummern ändern (s. Abschnitt "Portnummer der Verbindung des Geräts ändern" auf S. 97).

Schritt 7. Benutzerkonto auswählen

Geben Sie das Domain-Benutzerkonto des Benutzers an, unter dem mithilfe von QR-Codes Installationspakete auf die mobilen Geräte der Benutzer heruntergeladen werden.
Das Benutzerkonto muss im Format *<Domain-Name>\<Kontoname>* angegeben werden.

Über die Schaltfläche **Test** können Sie die Verbindung mit dem Administrationsserver prüfen.

Schritt 8. Installation der Kaspersky Security Center 10 Web Console starten

Klicken Sie auf die Schaltfläche **Installieren**, um die Installation von Kaspersky Security Center 10 Web Console zu starten.

Der Installationsvorgang wird im Fenster des Assistenten angezeigt.

Schritt 9. Installation der Kaspersky Security Center 10 Web Console beenden

Wenn ein Apache Server Version 2.4.25 oder höher auf dem Gerät bereits installiert wurde oder die automatische Installation des Apache-Servers fehlerhaft beendet wurde, wird Ihnen in diesem Schritt des Assistenten für die Installation von Kaspersky Security Center 10 Web Console vorgeschlagen, die Datei mit den Anweisungen zur Konfiguration des Apache-Servers zu öffnen. Um die Datei mit den Anweisungen nach Abschluss des Assistenten zu öffnen, aktivieren Sie das Kontrollkästchen **Die Datei readme.txt öffnen**.

Um den Installationsassistenten abzuschließen, klicken Sie auf **Fertig**.

Update der vorherigen Version von Kaspersky Security Center 10 Web Console

Sie können Kaspersky Security Center 10 Web Console auf dem Gerät installieren, auf dem die Vorgängerversion von Kaspersky Security Center 10 Web Console installiert ist. Beim Update auf die Version 10 bleiben die Daten und Einstellungen der Vorgängerversion von Kaspersky Security Center 10 Web Console erhalten.

► *Gehen Sie folgendermaßen vor, um ein Update von Kaspersky Security Center 10 Web Console Version 9.0 auf Version 10 durchzuführen:*

Starten Sie die ausführbare Datei setup.exe für die Version 10.

Das Fenster **Installationsprogramm für Kaspersky Security Center 10 Web Console** des Installationsassistenten wird geöffnet. Folgen Sie den Anweisungen des Assistenten.

Es wird nicht empfohlen, die Ausführung des Installationsassistenten abzubrechen. Wenn der Update-Vorgang in der Installationsphase von Kaspersky Security Center 10 Web Console unterbrochen wird, kann das eine Beeinträchtigung der Funktionsfähigkeit von Kaspersky Security Center Web Console 9.0 zur Folge haben.

Erweiterte Einstellungen für Kaspersky Security Center 10 Web Console und Self Service Portal

Nach der Installation von Kaspersky Security Center 10 Web Console und Self Service Portal können Sie deren erweiterte Einstellungen konfigurieren:

- Dateien mit dem Text des Lizenzvertrags und häufig gestellten Fragen erstellen, die sich der Benutzer bei Zugriff auf Kaspersky Security Center 10 Web Console und Self Service Portal ansehen kann (s. Abschnitt "Datei des Lizenzvertrags und Datei mit häufig gestellten Fragen anpassen" auf S. 99).

- Logo Ihres Unternehmens zur Benutzeroberfläche von Kaspersky Security Center 10 Web Console und Self Service Portal hinzufügen (s. Abschnitt "Logo anpassen" auf S. 99).

Portnummer der Verbindung des Geräts ändern

► *Um die Portnummer 8080 der Verbindung des Geräts zu Kaspersky Security Center 10 Web Console zu ändern, gehen Sie wie folgt vor:*

1. Öffnen Sie die Datei httpd.conf, die sich im Arbeitsordner des Apache-Servers befindet.

   Beispiel: "<Laufwerk>:\Program Files (x86) \KSC Apache 2.4\Apache2.4\conf\httpd.conf".

2. Ersetzen Sie den Wert des Ports 8080 durch den gewünschten Port an drei Stellen:

   - Zeile 1: `Listen 8080`
   - Zeile 38: `<VirtualHost *:8080>`
   - Zeile 54: `RewriteCond %{SERVER_PORT} !^8080$`

3. Starten Sie den Dienst des Apache-Servers neu.

4. Starten Sie die Kaspersky Security Center 10 Web Console neu.

Beispiel:

Wenn Sie den Port 8080 mit 443 ersetzen möchten, müssen die Zeilen wie folgt verändert werden:

Zeile 1: `Listen 443`

Zeile 38: `<VirtualHost *:443>`

Zeile 54: `RewriteCond %{SERVER_PORT} !^443$`

► *Um die Portnummer 8081 der Verbindung des Geräts zum Self Service Portal zu ändern, gehen Sie wie folgt vor:*

1. Öffnen Sie die Datei httpd.conf, die sich im Arbeitsordner des Apache-Servers befindet.

   Beispiel: "<Laufwerk>:\Program Files (x86) \KSC Apache 2.4\Apache2.4\conf\httpd.conf" with notepad++

2. Ersetzen Sie den Wert des Ports 8081 durch den gewünschten Port an drei Stellen:

   - Zeile 2: `Listen 8081`
   - Zeile 139: `<VirtualHost *:8081>`
   - Zeile 149: `RewriteCond %{SERVER_PORT} !^8081$`

3. Starten Sie den Dienst des Apache-Servers neu.

4. Starten Sie das Self Service Portal neu.

Es ist nicht empfehlenswert, den Port 80 für die Verbindung der Geräte mit Kaspersky Security Center 10 Web Console oder zu Self Service Portal zu verwenden, da der Port 80 für das Protokoll HTTP standardmäßig ernannt ist, und für die Verbindung der Geräte mit Kaspersky Security Center 10 Web Console und zu Self Service Portal wird das Protokoll HTTPS verwendet.

Datei des Lizenzvertrags und Datei mit häufig gestellten Fragen anpassen

► *Damit der Text des Lizenzvertrags und die Antworten auf häufig gestellte Fragen der Benutzer in der Benutzeroberfläche der Kaspersky Security Center 10 Web Console und/oder in der Benutzeroberfläche des Self Service Portals verfügbar sind, gehen Sie wie folgt vor:*

1. Legen Sie eine Datei des Lizenzvertrags (eula.txt oder eula.html) und eine Datei mit Antworten auf häufig gestellte Fragen (faq.txt oder faq.html) an.

2. Verschieben Sie die erstellten Dateien in den Installationsordner des Apache-Servers in den Unterordner htdocs\help.

Die Texte des Lizenzvertrags und die Antworten auf häufig gestellte Fragen sind dann über Links aus dem Hauptfenster von Kaspersky Security Center 10 Web Console und/oder dem Hauptfenster des Self Service Portals verfügbar.

Logo anpassen

► *Damit das Logo Ihres Unternehmens in der Benutzeroberfläche der Kaspersky Security Center 10 Web Console und/oder in der Benutzeroberfläche des Self Service Portals angezeigt wird, gehen Sie folgendermaßen vor:*

1. Stellen Sie die Logo-Datei bereit, die folgende Voraussetzungen erfüllen muss:
   - Dateiformat: PNG
   - Dateiname: logo.png
   - Größe des Logos: 220×72 Pixel.
2. Verschieben Sie die Logo-Datei in den Installationsordner des Apache-Servers:
   - Wenn der Apache-Server unter Microsoft Windows installiert wurde, ist der Standardpfad des Installationsordners C:\Programmes\Apache Software Foundation\Apache2.2\htdocs\images\custom_logo.
   - Wenn der Apache-Server unter Linux installiert wurde, ist der Standardpfad des Installationsverzeichnisses /opt/kaspersky/kscwebconsole/share/htdocs/images/custom_logo.

Konfiguration des Antiviren-Schutzsystems im Netzwerk eines Kundenunternehmens

In diesem Abschnitt werden die Besonderheiten der Konfiguration des Antiviren-Schutzes über die Verwaltungskonsole im Netzwerk eines Kundenunternehmens beschrieben.

Die Konfiguration des Antiviren-Schutzes ist ein Teil des Vorgangs der Softwareverteilung im Netzwerk eines Kundenunternehmens. Der Konfigurationsvorgang des Antiviren-Schutzes umfasst folgende Schritte:

1. Gerät auswählen, das die Rolle des Update-Agenten im Netzwerk des Kundenunternehmens übernehmen soll.
2. Administrationsagenten lokal auf dem als Update-Agent ausgewählten Gerät installieren.
3. Remote-Installation des Administrationsagenten und der erforderlichen Kaspersky Lab-Programme auf den Geräten des Kundenunternehmens.

   In diesem Abschnitt werden die erforderlichen Bedingungen für die Remote-Installation von Programmen auf den Geräten des Kundenunternehmens erläutert.
   Die Remote-Installation des Administrationsagenten und der Antiviren-Programme von Kaspersky Lab wird ausführlich im Abschnitt Remote-Installation von Programmen beschrieben (s. S. 108).
4. Hierarchie der Administrationsgruppen erstellen, die dem virtuellen Administrationsserver untergeordnet sind.

In diesem Abschnitt

Gerät zum Update-Agenten bestimmen. Update-Agenten konfigurieren

Sie können die Geräte des Kundenunternehmens, die über keine direkte Verbindung mit dem virtuellen Administrationsserver verfügen, über ein Verbindungs-Gateway verwalten.

Ferner können Sie ein Gerät manuell als Update-Agent für die Administrationsgruppe festlegen und in der Verwaltungskonsole als Verbindungs-Gateway konfigurieren.

► *Um ein Gerät zum Update-Agenten der Administrationsgruppe zu bestimmen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Node Administrationsserver.
2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftsfenster des Administrationsservers im Abschnitt **Update-Agenten** aus und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird das Fenster **Update-Agenten hinzufügen** geöffnet.

4. Gehen Sie im Fenster **Update-Agenten hinzufügen** wie folgt vor:

    a. Wählen Sie das Gerät, das die Rolle des Update-Agenten übernehmen soll, indem Sie die Liste durch Klicken auf die Schaltfläche  öffnen, die sich rechts neben der Schaltfläche **Hinzufügen** befindet. Es sind folgende Methoden für das Hinzufügen von Geräten verfügbar:

- **Gerät aus der Gruppe hinzufügen**. Gerät aus dem Ordner **Verwaltete Geräte** hinzufügen.
- **Verbindungs-Gateway in der demilitarisierten Zone nach Adresse hinzufügen**. Adresse des Verbindungs-Gateways angeben.

Verwenden Sie diese Variante, um als Update-Agent ein Gerät hinzuzufügen, das durch eine Firewall geschützt wird, da dieses Gerät nicht direkt in eine Administrationsgruppe aufgenommen werden kann.

Berücksichtigen Sie bei der Auswahl des Geräts die Besonderheiten des Update-Agenten und die Anforderungen an das Gerät, das die Rolle des Update-Agenten übernehmen soll.

    b. Geben Sie eine Reihe von Geräten an, auf die der Update-Agent Updates verteilen soll. Sie können dazu die Administrationsgruppe oder das Subnet Network Location Awareness (NLA-Subnet) angeben.

5. Klicken Sie auf die Schaltfläche **OK**.

Der hinzugefügte Update-Agent wird in der Liste der Update-Agenten im Abschnitt **Update-Agenten** angezeigt.

Das erste Gerät mit installiertem Administrationsagenten, das eine Verbindung zum virtuellen Server herstellt, wird automatisch zum Update-Agenten bestimmt und als Verbindungs-Gateway konfiguriert.

Nachdem der Update-Agent hinzugefügt wurde, wird er vom Administrationsserver bei einer regelmäßigen Netzwerkabfrage nach seiner IP-Adresse erkannt und in den Ordner **Nicht zugeordnete Geräte** verschoben. Da der Update-Agent durch die Firewall geschützt wird, ist es erforderlich, folgende Aktionen auszuführen, um seine Einstellungen anzupassen:

1. Fügen Sie dieses Gerät zur ausgewählten Administrationsgruppe hinzu.
2. Öffnen Sie das Eigenschaftenfenster des Administrationsservers im Abschnitt **Update-Agenten** erneut.
3. Entfernen Sie das nach Adresse hinzugefügte Gerät aus der Liste der Update-Agenten.
4. Fügen Sie dieses Gerät aus dem Ordner **Verwaltete Geräte** hinzu, indem Sie auf die Schaltfläche **Hinzufügen** oder **Gerät aus der Gruppe hinzufügen** klicken.
5. Überprüfen Sie im Eigenschaftsfenster des Update-Agenten im Abschnitt **Erweitert**, ob die Kontrollkästchen **Verbindungs-Gateway** und **Verbindungsaufbau mit dem Gateway durch den Administrationsserver auslösen (wird verwendet, wenn das Gateway sich in einer entmilitarisierten Zone befindet)** aktiviert sind.

Administrationsagenten lokal auf dem als Update-Agent ausgewählten Gerät installieren

Damit das Gerät, das als Update-Agent ausgewählt wurde, direkt mit dem virtuellen Administrationsserver verbunden werden kann, um die Rolle des Verbindungs-Gateway zu übernehmen, ist es erforderlich, den Administrationsagenten lokal auf diesem Gerät zu installieren.

Die Reihenfolge der lokalen Installation des Administrationsagenten auf dem Gerät, das als Update-Agent ausgewählt wurde, stimmt mit der Reihenfolge der lokalen Installation des Administrationsagenten auf jedem Gerät im Netzwerk überein.

Für das Gerät, das als Update-Agent ausgewählt wurde, müssen folgende Bedingungen erfüllt sein:

- Bei der lokalen Installation des Administrationsagenten muss im Fenster des Installationsassistenten **Administrationsserver** im Feld **Serveradresse** die Adresse des virtuellen Administrationsservers angegeben werden, der das Gerät verwaltet. Als Adresse des Geräts können Sie die IP-Adresse oder den Namen des Geräts im Windows-Netzwerk angeben.

  Geben Sie die Adresse des virtuellen Servers auf folgende Weise an: **<Vollständige Adresse des physikalischen Administrationsservers, dem der virtuelle Server untergeordnet ist>/<Name des virtuellen Administrationsservers>**.

- Damit das Gerät als Verbindungs-Gateways funktionieren kann, müssen alle Ports auf dem Gerät geöffnet sein, die für die Verbindung mit dem Administrationsserver erforderlich sind.

Aufgrund der Installation des Administrationsagenten mit den vorgegebenen Einstellungen auf dem Gerät führt Kaspersky Security Center automatisch die folgenden Aktionen aus:

- Nimmt das Gerät in die Gruppe **Verwaltete Geräte** des virtuellen Administrationsservers auf.

- Ernennt dieses Gerät zum Update-Agenten der Gruppe **Verwaltete Geräte** des virtuellen Administrationsservers.

Es ist erforderlich und ausreichend, den Administrationsagenten lokal auf einem Gerät zu installieren, das zum Update-Agenten der Gruppe **Verwaltete Geräte** im Unternehmensnetzwerk ernannt wurde. Sie können den Administrationsagenten von einem entfernten Standort auf jene Geräte installieren, die als Update-Agenten in den untergeordneten Administrationsgruppen fungieren. Verwenden Sie dabei den Update-Agenten der Gruppe **Verwaltete Geräte** als Verbindungs-Gateway.

Siehe auch:

Lokale Installation des Administrationsagenten 139

Remote-Installation von Programmen 108

Erforderliche Bedingungen für die Installation von Programmen auf den Geräten des Kundenunternehmens

Der Vorgang zur Remote-Installation von Programmen auf den Geräten eines Kundenunternehmens stimmt mit dem Vorgang zur Remote-Installation von Programmen innerhalb des Unternehmens überein (s. Abschnitt "Remote-Installation von Programmen" (s. S. 108)).

Zur Installation von Programmen auf den Geräten eines Kundenunternehmens müssen die folgenden Bedingungen erfüllt sein:

- Vor der Erstinstallation von Programmen auf den Geräten des Kundenunternehmens ist es erforderlich, den Administrationsagenten auf den Geräten zu installieren.

  Bei der Konfiguration des Installationspakets für den Administrationsagenten auf der Seite des Dienstanbieters ist es erforderlich, im Eigenschaftenfenster des Installationspakets im Programm Kaspersky Security Center folgende Einstellungen anzupassen:

  - Geben Sie im Abschnitt **Verbindung** in der Zeile **Serveradresse** dieselbe Adresse des virtuellen Administrationsservers wie bei der lokalen Installation des Administrationsagenten auf dem Update-Agenten an.

  - Aktivieren Sie im Abschnitt **Erweitert** das Kontrollkästchen **Eine Verbindung mit dem Administrationsserver über das Verbindungs-Gateway herstellen**. Geben Sie in der Zeile **Adresse des Verbindungs-Gateways** die Adresse des Update-Agenten an. Als Adresse des Geräts können Sie die IP-Adresse oder den Namen des Geräts im Windows-Netzwerk angeben.

- Wählen Sie als Methode zum Laden des Installationspakets für den Administrationsagenten **Mit Betriebssystem-Mitteln mithilfe von Update-Agenten** aus. Die Auswahl der Methode zum Laden des Pakets erfolgt auf folgende Weise:

- Bei der Installation von Programmen mit der Aufgabe zur Remote-Installation können Sie die Methode zum Laden des Installationspakets folgendermaßen auswählen:
  - beim Erstellen der Aufgabe zur Remote-Installation im Fenster **Einstellungen**;
  - im Eigenschaftenfenster der Aufgabe zur Remote-Installation im Abschnitt **Einstellungen**.
- Bei der Installation von Programmen mit dem Assistenten zur Remote-Installation können Sie die Methode zum Laden des Installationspakets im Fenster des Assistenten **Einstellungen** auswählen.

- Das Benutzerkonto, unter dem der Update-Agent funktioniert, muss über Zugriff auf die Ressource Admin$ auf den Client-Geräten verfügen.

Hierarchie der Administrationsgruppen erstellen, die dem virtuellen Administrationsserver untergeordnet sind

Nachdem der virtuelle Administrationsserver erstellt wurde, enthält er nur die Administrationsgruppe **Verwaltete Geräte**.

Der Vorgang zum Erstellen einer Hierarchie der dem virtuellen Administrationsserver untergeordneten Administrationsgruppen stimmt mit dem Vorgang zum Erstellen einer Hierarchie der Administrationsgruppen überein, die dem physikalischen Administrationsserver untergeordnet sind. Eine Beschreibung für diesen Vorgang finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

> Den Administrationsgruppen, die dem virtuellen Administrationsserver untergeordnet sind, können Sie keine untergeordneten und virtuellen Administrationsserver hinzufügen. Dies wird durch die Einschränkungen der virtuellen Administrationsserver verursacht, die im *Administratorhandbuch zu Kaspersky Security Center* beschrieben werden.

Remote-Installation von Programmen

In diesem Abschnitt werden Methoden für die Remote-Installation bzw. Deinstallation von Kaspersky Lab-Programmen auf Netzwerkgeräten beschrieben.

> Bevor die Installation der Programme auf den Client-Geräten beginnt, müssen Sie sich vergewissern, dass die Hardware- und Softwarevoraussetzungen das Gerät den Anforderungen entsprechen.

In diesem Abschnitt wird die Remote-Installation von Programmen über die Verwaltungskonsole beschrieben.

Die Kommunikation des Administrationsservers mit den Client-Geräten wird durch den Administrationsagenten sichergestellt. Deshalb ist es erforderlich, den Administrationsagenten auf jedem Client-Gerät zu installieren, das mit dem System der zentralen Remote-Administration verbunden werden soll.

> Auf dem Gerät, auf dem der Administrationsserver installiert wurde, kann nur die Serverversion des Administrationsagenten verwendet werden. Sie gehört zum Administrationsserver und wird zusammen mit ihm installiert und deinstalliert. Der Administrationsagent muss auf diesem Gerät nicht installiert werden.

Der Administrationsagent wird genauso wie die Anwendungen installiert. Dabei kann die Installation im Remote-Betrieb oder lokal erfolgen. Bei einer zentralen Installation von Antiviren-Programmen über die Verwaltungskonsole können Sie den Administrationsagenten zusammen mit den Antiviren-Programmen installieren.

Die Administrationsagenten können sich je nach den Kaspersky-Lab-Anwendungen unterscheiden, für die sie installiert sein müssen. In einigen Fällen ist nur eine lokale Installation des Administrationsagenten möglich (für Details siehe die Handbücher der jeweiligen Anwendung). Der Administrationsagent wird einmal auf dem Client-Gerät installiert.

Die Verwaltung von Kaspersky-Lab- Programmen über die Verwaltungskonsole erfolgt mit Verwaltungs-Plug-ins. Deshalb muss das Verwaltungs-Plug-in für Kaspersky Security Center auf dem Administrator-Arbeitsplatz installiert werden, um dieses Programm verwalten zu können.

Sie können eine Remote-Installation von Programmen vom Administrator-Arbeitsplatz aus im Programmhauptfenster von Kaspersky Security Center ausführen.

> Einige Kaspersky Lab-Programme lassen sich auf Client-Geräten nur lokal installieren (für Details siehe die Handbücher der entsprechenden Programme). Die Remote-Verwaltung dieser Programme mithilfe von Kaspersky Security Center ist verfügbar.

Um Programme im Remote-Betrieb zu installieren, erstellen Sie eine Aufgabe zur Remote-Installation.

Die angelegte Aufgabe zur Remote-Installation wird je nach dem eingestellten Zeitplan aufgerufen. Sie können den Installationsvorgang unterbrechen, indem Sie die Aufgabe manuell beenden.

> Wenn die Remote-Installation eines Programms fehlerhaft abgeschlossen wird, können Sie prüfen, wodurch das Problem hervorgerufen wurde, und es mithilfe des Tools Vorbereitung des Geräts auf Remote-Installation beseitigen (s. Abschnitt "Vorbereitung des Geräts auf Remote-Installation. Tool riprep.exe" auf S. 131).

Sie können den Fortschritt des Installationsvorgangs der Schutzprogramme von Kaspersky Lab im Netzwerk mithilfe des Berichts über die Softwareverteilung verfolgen.

Kaspersky Security Center unterstützt die Remote-Administration für folgende Kaspersky-Lab-Anwendungen:

- Für Workstations:
  - Kaspersky Endpoint Security 10 für Windows (unterstützt alle Versionen)
  - Kaspersky Endpoint Security 8 für Linux (unterstützt alle Versionen)
  - Kaspersky Endpoint Security 10 für Linux (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)
  - Kaspersky Endpoint Security 8 for Mac (unterstützt alle Versionen)

- Kaspersky Endpoint Security 10 für Mac (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)
- Kaspersky Embedded Systems Security für Windows (geplante Veröffentlichung im November 2016).

- Für mobile Geräte:
  - Kaspersky Security 10 für mobile Endgeräte (Installation bei Aktivierung der Funktion Mobile Geräte verwalten verfügbar).
- Für Dateiserver:
  - Kaspersky Endpoint Security 10 für Windows (unterstützt alle Versionen)
  - Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition (unterstützt alle Versionen)
  - Kaspersky Security 10 für Windows Server (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)
  - Kaspersky Anti-Virus 8.0 für Linux File Server (unterstützt alle Versionen)
  - Kaspersky Anti-Virus 10 für Linux File Server (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016).
- Für virtuelle Maschinen:
  - Kaspersky Security für Virtualisierung 3.0 Agentless
  - Kaspersky Security für virtuelle Umgebungen 3.0. Light Agent (unterstützt alle Versionen).
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Nodes.

Informationen über die neuesten Programmversionen erhalten Sie auf der Website des Technischen Supports auf der Seite von Kaspersky Security Center, im Abschnitt Allgemeine Infos (http://support.kaspersky.com/de/12029).

Detaillierte Informationen zur Verwaltung der aufgeführten Anwendungen über Kaspersky Security Center finden Sie in den Handbüchern der entsprechenden Anwendungen.

In diesem Abschnitt

Programme mit der Aufgabe zur Remote-Installation installieren

Kaspersky Security Center ermöglicht es, Programme auf den Geräten per Remote-Zugriff mithilfe der Aufgaben der Remote-Installation zu installieren. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Geräte auswählen, die vom Administrationsserver im Netzwerk gefunden wurden**. In diesem Fall wird die Aufgabe bestimmten Geräten zugewiesen. In diese Geräteauswahl können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

- **Geräteadressen manuell festlegen oder aus einer Liste importieren**. Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

- **Aufgabe zur Geräteauswahl festlegen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine standardmäßig erstellte Auswahl oder Ihre eigene Auswahl angeben.

- **Aufgabe der Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

Für eine korrekte Ausführung der Aufgabe der Remote-Installation auf einem Gerät, auf dem der Administrationsagent nicht installiert ist, müssen die folgenden Ports geöffnet werden: TCP 139 und 445 sowie UDP 137 und 138. Diese Ports sind standardmäßig auf allen Geräten geöffnet, die zur Domäne gehören. Sie werden automatisch mit dem Tool Vorbereitung des Geräts zur Remote-Installation geöffnet (s. Abschnitt "Vorbereitung des Geräts zur Remote-Installation. Tool riprep.exe" auf S. 131).

In diesem Abschnitt

Programm auf ausgewählten Geräten installieren

► *Um ein Programm auf ausgewählten Geräten zu installieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten Geräte verwaltet.

2. Wahlen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

3. Starten Sie den Vorgang zur Erstellung der Aufgabe, indem Sie auf den Link **Aufgabe erstellen** klicken.

Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen.

Wählen Sie im Fenster **Aufgabentyp** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** den Aufgabentyp **Remote-Installation des Programms** aus.

Nach Abschluss des Assistenten für die Erstellung einer Aufgabe wird die Aufgabe zur Remote-Installation des gewählten Programms für die ausgewählten Geräte erstellt. Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsplatz des Ordners **Aufgaben** angezeigt.

4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm auf den gewählten Geräten installiert.

Programm auf den Client-Geräten einer Administrationsgruppe installieren

► *Um ein Programm auf Client-Geräten einer Administrationsgruppe zu installieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zu dem Administrationsserver her, der die gewünschte Administrationsgruppe verwaltet.

2. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.

3. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Aufgaben** aus.

4. Starten Sie den Vorgang zur Erstellung der Aufgabe, indem Sie auf den Link **Aufgabe erstellen** klicken.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen.

Wählen Sie im Fenster **Aufgabentyp** des Assistenten für das Erstellen einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** den Aufgabentyp **Remote-Installation des Programms** aus.

Nach Abschluss des Assistenten für die Erstellung einer Aufgabe wird die Gruppenaufgabe zur Remote-Installation des gewählten Programms erstellt. Die erstellte Aufgabe wird im Arbeitsplatz der Administrationsgruppe auf der Registerkarte **Aufgaben** angezeigt.

5. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm auf den Client-Geräten der Administrationsgruppe installiert.

Programme mit Gruppenrichtlinien des Active Directory installieren

Mit Kaspersky Security Center können Sie Programme von Kaspersky Lab mithilfe der Gruppenrichtlinien des Active Directory installieren.

> Die Installation von Programmen mit Gruppenrichtlinien des Active Directory ist nur möglich, wenn Installationspakete verwendet werden, die den Administrationsagenten enthalten.

► *Um ein Programm mithilfe von Gruppenrichtlinien des Active Directory zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die Erstellung der Gruppenaufgabe für Remote-Installation oder der Aufgabe für Remote-Installation für bestimmte Geräte.

2. Aktivieren Sie im Fenster **Einstellungen** des Assistenten für die Erstellung einer Aufgabe das Kontrollkästchen **Installation des Installationspakets in Gruppenrichtlinien des Active Directory festlegen**.

3. Starten Sie die erstellte Aufgabe zur Remote-Installation manuell oder gemäß einem Zeitplan.

Daraufhin wird die Remote-Installation auf folgende Weise ausgeführt:

1. Nach dem Start der Aufgabe werden in jeder Domäne, zu der Client-Geräte für diese Aufgabe zur Remote-Installation gehören, folgende Objekte angelegt:

   - Gruppenrichtlinie mit dem Namen **Kaspersky_AK{GUID}**

   - mit der Gruppenrichtlinie verbundene Sicherheitsgruppe **Kaspersky_AK{GUID}** Diese Sicherheitsgruppe umfasst Client-Geräte, auf die sich die Aufgabe erstreckt. Die Zusammensetzung der Sicherheitsgruppe bestimmt den Geltungsbereich der Gruppenrichtlinie.

2. Die Installation der Programme auf Client-Geräten erfolgt direkt aus dem freigegebenen Netzwerkordner Share. Im Installationsordner von Kaspersky Security Center wird dabei ein untergeordneter Hilfsordner erstellt, der die msi-Datei für das zu installierende Programm enthält.

3. Beim Hinzufügen neuer Geräte zum Gültigkeitsbereich der Aufgabe werden diese erst beim nächsten Start der Aufgabe zur entsprechenden Sicherheitsgruppe hinzugefügt. Wenn das Kontrollkästchen **Übersprungene Aufgaben starten** aktiviert ist, werden die Geräte sofort zur Sicherheitsgruppe hinzugefügt.

4. Beim Löschen von Geräten aus dem Gültigkeitsbereich einer Aufgabe werden sie erst beim nächsten Start der Aufgabe aus der Sicherheitsgruppe gelöscht.

5. Beim Löschen der Aufgabe aus dem Active Directory werden die Richtlinie, der Link auf die Richtlinie und die mit der Aufgabe verbundene Sicherheitsgruppe gelöscht.

Wenn Sie ein anderes Installationsschema über Active Directory verwenden möchten, können Sie die Einstellungen manuell ändern. Das kann in folgenden Fällen nötig werden:

- wenn der Administrator für Antiviren-Sicherheit nicht die nötigen Rechte besitzt, um im Active Directory einiger Domänen Änderungen vorzunehmen;

- wenn das ursprüngliche Programmpaket auf einer separaten Netzwerkressource gespeichert werden soll;

- wenn eine Gruppenrichtlinie konkreten Unterabteilungen des Active Directory zugewiesen werden soll.

Folgende alternative Installationsschemata über Active Directory sind verfügbar:

- Falls die Installation direkt aus dem freigegebenen Ordner von Kaspersky Security Center erfolgen muss, muss in den Eigenschaften der Gruppenrichtlinie des Active Directory eine msi-Datei angegeben werden, die sich im untergeordneten exec-Ordner des Ordners des Installationspakets für das erforderliche Programm befindet.

- Wenn das Installationspaket in einer anderen Netzwerkressource gespeichert werden muss, kopieren Sie den ganzen Inhalt des Ordners exec in das Paket, weil der Ordner neben der msi-Datei die Konfigurationsdateien enthält, die beim Anlegen des Installationspakets erstellt wurden. Um den Schlüssel zusammen mit dem Programm zu installieren, kopieren Sie auch die Schlüsseldatei in den Ordner.

Programme auf untergeordneten Administrationsservern installieren

► *Um ein Programm auf untergeordneten Administrationsservern zu installieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten untergeordneten Administrationsserver verwaltet.

2. Vergewissern Sie sich, dass sich das zum Programm passende Installationspaket auf jedem der gewählten untergeordneten Administrationsserver befindet.
   Wenn das Installationspaket auf einem der untergeordneten Server nicht vorhanden ist, verteilen Sie es mithilfe der Aufgabe Verteilung des Installationspakets (s. Abschnitt "Verteilung von Installationspaketen auf untergeordneten Administrationsservern" auf S. 126).

3. Starten Sie das Erstellen einer Aufgabe zur Installation eines Programms auf untergeordneten Administrationsservern auf eine der folgenden Weisen:

   - Wenn Sie eine Aufgabe für untergeordnete Server einer gewählten Administrationsgruppe erstellen möchten, starten Sie das Erstellen einer Gruppenaufgabe zur Remote-Installation für diese Gruppe (s. Abschnitt "Programm auf Client-Geräten einer Administrationsgruppe installieren" auf S. 113).

- Wenn Sie eine Aufgabe für eine Auswahl von untergeordneten Servern erstellen möchten, starten Sie das Erstellen einer Aufgabe zur Remote-Installation für eine Reihe von Geräten (s. Abschnitt "Programm auf ausgewählten Geräten installieren" auf S. 112).

Daraufhin wird der Assistent für das Erstellen einer Aufgabe zur Remote-Installation gestartet. Folgen Sie den Anweisungen.

Wählen Sie im Fenster **Aufgabentyp** des Assistenten für die Erstellung einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Remote-Installation des Programms auf den untergeordneten Administrationsservern** aus.

Nach Abschluss des Assistenten für die Erstellung einer Aufgabe wird die Aufgabe zur Remote-Installation des gewählten Programms auf den gewählten untergeordneten Administrationsservern erstellt.

4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm auf den gewählten untergeordneten Administrationsservern installiert.

Programme mit dem Assistenten zur Remote-Installation installieren

Bei der Installation von hauseigenen Programmen können Sie den Assistenten zur Remote-Installation einsetzen. Der Assistent zur Remote-Installation ermöglicht die Remote-Installation der Programme mit zuvor angelegten Installationspaketen oder von den Programmpaketen.

Damit die Aufgabe Remote-Installation auf einem Client-Gerät, auf dem der Administrationsagent nicht installiert ist, korrekt ausgeführt wird, müssen die folgenden Ports geöffnet werden: a) TCP 139 und 445; b) UDP 137 und 138. Diese Ports sind standardmäßig für alle Geräte geöffnet, die zur Domäne gehören, und werden automatisch mit dem Tool Vorbereitung des Geräts zur Remote-Installation geöffnet (s. Abschnitt "Vorbereitung des Geräts zur Remote-Installation. Tool riprep.exe" auf S. 131).

► *Um ein Programm mithilfe des Assistenten zur Remote-Installation zu installieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zu dem Administrationsserver her, der die gewünschte Administrationsgruppe verwaltet.

2. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.

3. Klicken Sie im Arbeitsplatz der Gruppe auf die Schaltfläche **Aktion ausführen** und wählen Sie in der Dropdown-Liste den Punkt **Programm installieren** aus.

   Daraufhin wird der Assistent zur Remote-Installation gestartet. Folgen Sie den Anweisungen.

4. Klicken Sie im letzten Schritt des Assistenten auf die Schaltfläche **Weiter**, um die Aufgabe zur Remote-Installation auf den gewählten Geräten zu erstellen und zu starten.

Als Ergebnis der Ausführung des Assistenten zur Remote-Installation führt Kaspersky Security Center folgende Aktionen aus:

- Erstellt ein Installationspaket für das Programm (wenn es zuvor nicht erstellt wurde). Das Installationspaket wird im Ordner **Remote-Installation** im Unterordner **Installationspakete** mit dem Namen gespeichert, der dem Namen und der Version des Programms entspricht. Dieses Installationspaket kann zur weiteren Installation des Programms herangezogen werden.

- Erstellt und startet eine Aufgabe zur Remote-Installation für eine Reihe von Geräten oder für eine Administrationsgruppe. Die erstellte Aufgabe zur Remote-Installation wird im Ordner **Aufgaben** abgelegt und zu den Aufgaben der Administrationsgruppe hinzugefügt, für die sie erstellt wurde. Später können Sie diese Aufgabe manuell starten.
  Der Aufgabenname entspricht dem Namen des Installationspakets für die Installation des Programms: **Installation <Name des Installationspakets>**.

Bericht über die Verteilung von Schutz-Software anzeigen

Um die Softwareverteilung im Netzwerk zu verfolgen, nutzen Sie den Bericht über die Verteilung von Schutz-Software.

► *Um den Bericht über die Verteilung von Schutz-Software anzuzeigen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.
2. Wählen Sie im Arbeitsplatz des Knotens die Registerkarte **Berichte** aus.
3. Wählen Sie im Arbeitsplatz der Registerkarte **Berichte** die Berichtsvorlage **Bericht über die Verteilung von Schutz-Software** aus.

Im Arbeitsplatz wird daraufhin ein Bericht erstellt, der Daten über die Softwareverteilung auf allen Geräten des Netzwerks enthält.

Sie können einen neuen Bericht über die Verteilung von Schutz-Software erstellen und angeben, welche Art von Daten darin enthalten sein soll:

- für eine Administrationsgruppe
- für bestimmte Geräte
- für die Geräteauswahl
- für alle Geräte.

Detaillierte Informationen über das Erstellen eines neuen Berichts finden Sie im *Administratorhandbuch für Kaspersky Security Center*.

Im Rahmen von Kaspersky Security Center wird davon ausgegangen, dass der Schutz auf dem Gerät dann aktiv ist, wenn ein Schutzprogramm installiert und der Echtzeitschutz eingeschaltet ist.

Remote-Deinstallation von Programmen

Kaspersky Security Center ermöglicht es, Programme von den Geräten per Remote-Zugriff mithilfe der Aufgaben der Remote-Deinstallation zu deinstallieren. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Geräte auswählen, die vom Administrationsserver im Netzwerk gefunden wurden**. In diesem Fall wird die Aufgabe bestimmten Geräten zugewiesen. In diese Geräteauswahl können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

- **Geräteadressen manuell festlegen oder aus einer Liste importieren**. Sie können NetBIOS-Namen, DNS-Namen, IP-Adressen sowie IP-Adressbereiche der Geräte festlegen, denen eine Aufgabe zugewiesen werden soll.

- **Aufgabe zur Geräteauswahl festlegen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine standardmäßig erstellte Auswahl oder Ihre eigene Auswahl angeben.

- **Aufgabe der Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

In diesem Abschnitt

Remote-Deinstallation eines Programms von den Client-Geräten einer Administrationsgruppe

► *Um ein Programm von den Client-Geräten einer Administrationsgruppe im Remote-Betrieb zu deinstallieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zu dem Administrationsserver her, der die gewünschte Administrationsgruppe verwaltet.

2. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe aus.

3. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Aufgaben** aus.

4. Starten Sie den Vorgang zur Erstellung der Aufgabe, indem Sie auf den Link **Aufgabe erstellen** klicken.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen.

   Wählen Sie im Fenster **Aufgabentyp** des Assistenten für die Erstellung einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Remote-Deinstallation des Programms** aus.

   Nach Abschluss des Assistenten für die Erstellung einer Aufgabe wird die Gruppenaufgabe zur Remote-Deinstallation des gewählten Programms erstellt. Die erstellte Aufgabe wird im Arbeitsplatz der Administrationsgruppe auf der Registerkarte **Aufgaben** angezeigt.

5. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Deinstallation wird das gewählte Programm von den Client-Geräten der Administrationsgruppe entfernt.

Remote-Deinstallation eines Programms von den gewählten Geräten

► *Um ein Programm von den ausgewählten Geräten per Remote-Zugriff zu deinstallieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten Geräte verwaltet.

2. Wahlen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

3. Starten Sie den Vorgang zur Erstellung der Aufgabe, indem Sie auf die Schaltfläche **Aufgabe erstellen** klicken.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen.

   Wählen Sie im Fenster **Aufgabentyp** des Assistenten für die Erstellung einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Remote-Deinstallation des Programms** aus.

   Nach Abschluss des Assistenten für die Erstellung einer Aufgabe wird die Aufgabe zur Remote-Deinstallation des gewählten Programms für die ausgewählten Geräte erstellt. Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsplatz des Ordners **Aufgaben** angezeigt.

4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe zur Remote-Installation wird das gewählte Programm von den ausgewählten Geräten entfernt.

Verwendung von Installationspaketen

Beim Erstellen einer Aufgabe zur Remote-Installation werden Installationspakete eingesetzt, die die Einstellungen enthalten, die für die Installation eines Programms benötigt werden.

> Installationspakete können die Schlüsseldatei beinhalten. Es ist nicht empfehlenswert, die Installationspakete mit der Schlüsseldatei mit allgemeiner Leseberechtigung zu verteilen.

Sie können dasselbe Installationspaket mehrmals verwenden.

Die für den Administrationsserver erstellten Installationspakete liegen in der Konsolenstruktur im Ordner **Remote-Installation** im Unterordner **Installationspakete**. Auf dem Administrationsserver werden die Installationspakete im angegebenen gemeinsamen Ordner im Dienstordner Packages gespeichert.

In diesem Abschnitt

Installationspaket erstellen

► *Um ein Installationspaket zu erstellen, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** den Unterordner **Installationspakete** aus.

3. Starten Sie den Vorgang zum Erstellen eines Installationspakets auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf den Ordner **Installationspakete** und wählen Sie **Erstellen** → **Installationspaket**.
   - Klicken Sie mit der rechten Maustaste auf die Liste der Installationspakete und wählen Sie **Erstellen** → **Installationspaket**.
   - Klicken Sie im Block zur Verwaltung der Liste der Installationspakete auf den Link **Installationspaket erstellen**.

Daraufhin wird der Assistent für das Erstellen von Installationspaketen gestartet. Folgen Sie den Anweisungen.

Wenn ein Installationspaket für ein Kaspersky-Lab-Programm erstellt wird, kann Ihnen vorgeschlagen werden, den Lizenzvertrag für dieses Programm zu beachten. Lesen Sie den Endbenutzer-Lizenzvertrag sorgfältig. Wenn Sie mit allen Punkten des Vertrags einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**. Anschließend wird das Erstellen des Installationspakets fortgesetzt. Der Pfad der Datei mit dem Lizenzvertrag wird in einer Datei mit der Erweiterung kud oder kpd angegeben, die zum Lieferumfang des Programms gehört, für das ein Installationspaket erstellt wird.

> Beim Erstellen des Installationspakets für das Programm Kaspersky Endpoint Security für Mac können Sie die Sprache des Endbenutzer-Lizenzvertrags auswählen.

Bei der Erstellung eines Installationspakets für eines der Programme von Kaspersky Lab können Sie die automatische Installation der systemweiten Komponenten (Voraussetzungen) aktivieren, die für die Installation dieses Programms erforderlich sind. Der Assistent für das Erstellen von Installationspaketen zeigt die Liste aller systemweiten Komponenten für das gewählte Programm an. Wird ein Installationspaket für ein Patch (unvollständiges Programmpaket) erstellt, so enthält die Liste der systemweiten Komponenten alle für eine Verteilung des Patches erforderlichen Komponenten, einschließlich der Version mit dem vollständigen Programmpaket. Diese Liste kann später in den Eigenschaften des Installationspakets eingesehen werden.

Nach Abschluss des Assistenten wird das erstellte Installationspaket im Arbeitsplatz des Ordners **Installationspakete** in der Konsolenstruktur angezeigt.

Das Installationspaket für eine Remote-Installation des Administrationsagenten muss nicht manuell erstellt werden. Es wird automatisch bei der Installation von Kaspersky Security Center erstellt und liegt im Ordner **Installationspakete**. Wenn das Paket für die Remote-Installation des Administrationsagenten deinstalliert wurde, muss zum erneuten Anlegen als Beschreibungsdatei die Datei nagent10.kud ausgewählt werden, die im Ordner NetAgent im Lieferumfang von Kaspersky Security Center enthalten ist.

Geben Sie in den Einstellungen der Installationspakete die Daten der privilegierten Benutzerkonten nicht an.

Beim Erstellen des Installationspakets für den Administrationsserver muss als Beschreibungsdatei die Datei sc10.kud ausgewählt werden, die sich im Stammverzeichnis des Lieferumfangs von Kaspersky Security Center befindet.

Installationspakete auf untergeordnete Administrationsserver verteilen

► *Um Installationspakete auf untergeordnete Administrationsserver zu verteilen, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten untergeordneten Administrationsserver verwaltet.

2. Starten Sie das Erstellen einer Aufgabe zur Verteilung eines Installationspakets auf untergeordnete Administrationsserver auf eine der folgenden Weisen:

   - Wenn Sie die Aufgabe für untergeordnete Server einer gewählten Administrationsgruppe erstellen möchten, starten Sie das Erstellen einer Gruppenaufgabe für diese Gruppe.

   - Wenn Sie die Aufgabe für eine Auswahl der untergeordneten Server erstellen möchten, starten Sie das Erstellen einer Aufgabe für eine Reihe von Geräten.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen.

   Wählen Sie im Fenster **Aufgabentyp** des Assistenten für die Erstellung einer Aufgabe im Knoten **Kaspersky Security Center Administrationsserver** im Ordner **Erweitert** den Aufgabentyp **Verteilung des Installationspakets** aus.

   Nach Abschluss des Assistenten für die Erstellung einer Aufgabe wird die Aufgabe zur Verteilung der gewählten Installationspakete auf die gewählten untergeordneten Administrationsserver erstellt.

3. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen vorgegebenen Zeitplan gestartet wurde.

Nach Fertigstellung der Aufgabe werden die gewählten Installationspakete auf die gewählten untergeordneten Administrationsserver kopiert.

Installationspakete mithilfe von Update-Agenten verteilen

Für die Verteilung von Installationspaketen innerhalb einer Administrationsgruppe können Sie Update-Agenten verwenden.

Nach dem Download von Installationspaketen von dem Administrationsserver werden sie durch die Update-Agenten automatisch mit Multi-IP-Versand auf die Client-Geräte verteilt.
Der IP-Versand neuer Installationspakete im Rahmen einer Administrationsgruppe erfolgt einmal. Wenn ein Client-Gerät während des Versands vom Unternehmensnetzwerk getrennt wurde, lädt der Administrationsagent des Client-Geräts beim Aufgabenstart automatisch das benötigte Installationspaket vom Update-Agenten.

Daten über die Ergebnisse der Programminstallation an Kaspersky Security Center übertragen

Nachdem ein Installationspaket für das Programm erstellt wurde, können Sie das Installationspaket so anpassen, dass Diagnoseinformationen über die Ergebnisse der Programminstallation an Kaspersky Security Center übertragen werden.
Für Installationspakete für Kaspersky-Lab-Programme ist die Übertragung von Diagnoseinformationen über die Ergebnisse der Programminstallation standardmäßig angepasst. Es sind keine zusätzlichen Einstellungen erforderlich.

► *Um die Übertragung von Diagnosedaten über die Ergebnisse der Programminstallation an Kaspersky Security Center zu konfigurieren, gehen Sie wie folgt vor:*

1. Wechseln Sie in den Ordner des Installationspakets, das mit Kaspersky Security Center für die ausgewählte Anwendung angelegt wurde. Dieser Ordner liegt im gemeinsamen Ordner, der bei der Installation von Kaspersky Security Center angegeben wurde.

2. Öffnen Sie die Datei mit der Erweiterung kpd oder kud, um sie zu bearbeiten (beispielsweise mit dem Texteditor Notepad von Microsoft Windows).

   Die Datei weist das Format einer gewöhnlichen ini-Konfigurationsdatei auf.

3. Fügen Sie die folgenden Zeilen zu der Datei hinzu:

```
[SetupProcessResult]

Wait=1
```

Dieser Befehl konfiguriert Kaspersky Security Center so, dass es auf das Installationsende des Programms wartet, für welches Installationspaket erstellt wurde, und den Rückgabecode vom Installationsprogramm analysiert. Wenn die Übertragung der Diagnosedaten ausgeschaltet werden muss, setzen Sie den Wert des Schlüssels Wait auf 0.

4. Beschreiben Sie die Rückgabecodes für eine erfolgreiche Installation. Fügen Sie dazu in die Datei die folgenden Zeilen ein:

```
[SetupProcessResult_SuccessCodes]

<Rückgabecode>=[<Beschreibung>]

<Rückgabecode 1>=[<Beschreibung>]

  …
```

> Optionale Schlüssel stehen In eckigen Klammern.

Zeilensyntax:

- `<Rückgabecode>`: Beliebige Zahl, die dem Rückgabecode des Installationsprogramms entspricht. Es können beliebig viele Rückgabecodes eingegeben werden.
- `<Beschreibung>`. Textbeschreibung für das Ergebnis der Installation. Die Beschreibung kann fehlen.

5. Beschreiben Sie die Rückgabecodes für eine fehlerhafte Installation. Fügen Sie dazu in die Datei die folgenden Zeilen ein:

   ```
   [SetupProcessResult_ErrorCodes]

   <Rückgabecode>=[<Beschreibung>]

   <Rückgabecode 1>=[<Beschreibung>]

   …
   ```

   Die Zeilensyntax entspricht der Zeilensyntax für die Rückgabecodes bei einer erfolgreichen Installation.

6. Schließen Sie die kpd- oder kud-Datei, und speichern Sie die vorgenommenen Änderungen.

Die Informationen über die Ergebnisse der Installation des vom Benutzer angegebenen Programms werden in die Ereignisprotokolle von Kaspersky Security Center eingetragen und erscheinen in der Ereignisliste, in den Berichten und in den Ergebnissen der Aufgabenausführung.

Aktuelle Versionen der Programme downloaden

Kaspersky Security Center ermöglicht den Download von aktuellen Versionen der Programme für Unternehmen, die auf den Kaspersky-Lab-Internetservern zur Verfügung stehen.

► *Um aktuelle Versionen der Kaspersky-Lab-Programme für Unternehmen zu erhalten, gehen Sie wie folgt vor:*

1. Öffnen Sie das Hauptfenster von Kaspersky Security Center.

2. Öffnen Sie durch Klicken auf den Link **Es stehen neue Versionen der Kaspersky-Lab-Programme zur Verfügung** im Block **Softwareverteilung** das Fenster **Aktuelle Versionen der Programme**.

   Der Link **Es stehen neue Versionen der Kaspersky-Lab-Programme zur Verfügung** ist verfügbar, wenn der Administrationsserver eine neue Version eines Programms für Unternehmen auf dem Kaspersky-Lab-Internetserver erkennt.

3. Wählen Sie in der Liste das gewünschte Programm aus.

4. Laden Sie durch Klicken auf den Link in der Zeile **Webadresse der Programmdateien** das Programmpaket herunter.

   Wenn für das gewählte Programm die Schaltfläche **Programme herunterladen und Installationspakete erstellen** angezeigt wird, können Sie auf diese Schaltfläche klicken, damit das Programmpaket heruntergeladen und das Installationspaket automatisch erstellt wird. In diesem Fall wird das Programmpaket durch Kaspersky Security Center auf den Administrationsserver in den gemeinsamen Ordner heruntergeladen, der bei der Installation von Kaspersky Security Center vorgegeben wurde. Das automatisch erstellte Installationspaket wird im Ordner **Remote-Installation** der Konsolenstruktur im Unterordner **Installationspakete** angezeigt.

Nach dem Schließen des Fensters **Aktuelle Versionen der Programme** verschwindet der Link **Es stehen neue Versionen der Kaspersky-Lab-Programme zur Verfügung** im Block **Softwareverteilung**.

Sie können Installationspakete neuer Programmversionen erstellen und mit den erstellten Installationspaketen im Ordner **Remote-Installation** der Konsolenstruktur im Unterordner **Installationspakete** arbeiten.

Außerdem können Sie durch Klicken auf den Link **Aktuelle Versionen von Kaspersky-Lab-Programmen anzeigen** im Arbeitsplatz des Ordners **Installationspakete** das Fenster **Aktuelle Versionen der Programme** öffnen.

Siehe auch:

Vorbereitung des Geräts auf Remote-Installation. Tool riprep.exe

Die Remote-Installation einer Anwendung auf einem Client-Gerät kann aus den folgenden Gründen fehlerhaft beendet werden:

- Die Aufgabe wurde zuvor schon erfolgreich auf dem Gerät abgeschlossen. In diesem Fall muss sie nicht noch einmal ausgeführt werden.
- Beim Aufgabenstart war das Gerät ausgeschaltet. In diesem Fall muss das Gerät hochgefahren und die Aufgabe erneut gestartet werden.
- Es fehlt eine Verbindung zwischen dem Administrationsserver und dem Administrationsagenten, der auf dem Client-Gerät installiert ist. Zur Ursachenforschung können Sie das Tool Remote-Diagnose des Geräts (klactgui) verwenden. Detaillierte Informationen zur Verwendung des Tools finden Sie im *Administratorhandbuch für Kaspersky Security Center*.
- Wenn der Administrationsagent nicht auf dem Gerät installiert ist, können bei der Remote-Installation des Programms folgende Probleme auftreten:

- Auf dem Client-Gerät ist die Einstellung **Einfache Dateifreigabe** aktiv.
- Auf dem Client-Gerät wird der Dienst Server nicht ausgeführt.
- Auf dem Client-Gerät sind die Ports geschlossen.
- Die Berechtigungen des Benutzerkontos, unter dem die Aufgabe ausgeführt wird, reichen nicht aus.

Um Probleme zu lösen, die bei der Installation des Programms auf dem Client-Gerät aufgetreten sind, auf dem der Administrationsagent nicht installiert wurde, können Sie das Tool Vorbereitung des Geräts auf Remote-Installation (riprep) verwenden.

In diesem Abschnitt wird das Tool Vorbereitung des Geräts auf Remote-Installation beschrieben (riprep). Es wird im Installationsordner von Kaspersky Security Center auf dem Gerät mit dem installierten Administrationsserver gespeichert.

Das Tool Vorbereitung des Geräts auf Remote-Installation wird vom Betriebssystem Microsoft Windows XP Home Edition nicht unterstützt.

In diesem Abschnitt

Vorbereitung des Geräts auf Remote-Installation im interaktiven Modus

► *Um ein Gerät auf die Remote-Installation im interaktiven Modus vorzubereiten, gehen Sie wie folgt vor:*

1. Starten Sie auf dem Client-Gerät die Datei riprep.exe.

2. Aktivieren Sie im Hauptfenster des Tools Vorbereitung auf Remote-Installation die folgenden Kontrollkästchen:

   - **Deaktivieren des einfachen Zugriffs auf Dateien**
   - **Server-Dienst starten**
   - **Ports öffnen**
   - **Benutzerkonto hinzufügen**
   - **Benutzerkontensteuerung (UAC) deaktivieren**. Diese Einstellung ist für die Betriebssysteme Microsoft Windows Vista, Microsoft Windows 7 und Microsoft Windows Server 2008 verfügbar.

3. Klicken Sie auf die Schaltfläche **Starten**.

Daraufhin werden im unteren Bereich des Hauptfensters des Tools die Etappen der Vorbereitung des Geräts auf die Remote-Installation angezeigt.

Wenn Sie das Kontrollkästchen **Benutzerkonto hinzufügen** aktiviert haben, wird beim Erstellen des Benutzerkontos die Aufforderung zur Eingabe eines Namens für das Benutzerkonto und eines Kennworts angezeigt. Dadurch wird ein lokales, zur Gruppe lokaler Administratoren gehörendes Benutzerkonto angelegt.

Wenn Sie das Kontrollkästchen **Benutzerkontensteuerung (UAC) deaktivieren** aktiviert haben, wird auch dann versucht, die Benutzerkontensteuerung zu deaktivieren, wenn die Benutzerkontensteuerung bereits vor dem Start des Tools deaktiviert wurde. Nach dem Deaktivieren der Benutzerkontensteuerung erscheint auf dem Bildschirm die Aufforderung zum Neustart des Geräts.

Vorbereitung des Geräts auf Remote-Installation im nicht-interaktiven Modus

► *Um ein Gerät auf die Remote-Installation im nicht interaktiven Modus vorzubereiten,*

starten Sie auf dem Client-Gerät die Datei riprep.exe aus der Befehlszeile mit den gewünschten Schlüsseln.

Die Syntax des Tools lautet:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Die Schlüssel weisen folgende Bedeutung auf:

- `-silent` – Start des Tools im nicht interaktiven Modus
- `-cfg CONFIG_FILE` – Konfiguration des Tools definieren, wobei `CONFIG_FILE` der Pfad zur Konfigurationsdatei ist (Datei mit der Erweiterung .ini)
- `-tl traceLevel` – Eingeben der Ablaufverfolgungsebene, wobei `traceLevel` eine Zahl von 0 bis 5 sein kann. Wenn der Schlüssel nicht eingegeben wurde, wird der Wert 0 gesetzt.

Durch das Starten des Tools im nicht interaktiven Modus können Sie die folgenden Aufgaben ausführen:

- Einfache Dateifreigabe deaktivieren
- Dienst Server auf dem Client-Gerät starten
- Ports öffnen
- Benutzerkonto anlegen
- Benutzerkontensteuerung (UAC) deaktivieren.

Sie können die Einstellungen für die Vorbereitung des Geräts auf die Remote-Installation in der Konfigurationsdatei angeben, die mit dem Schlüssel `-cfg` vorgegeben wird. Um diese Einstellungen anzugeben, fügen Sie die folgenden Daten in die Konfigurationsdatei ein:

- Geben Sie im Abschnitt `Common` an, welche Aufgaben ausgeführt werden sollen:
  - `DisableSFS` – Einfachen Zugriff auf Dateien deaktivieren (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert)
  - `StartServer` – Dienst Server starten (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert)
  - `OpenFirewallPorts` – Alle nötigen Ports öffnen (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert)
  - `DisableUAC` – Benutzerkontensteuerung deaktivieren (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert)
  - `RebootType` – Verhalten beim erforderlichen Neustart beim Deaktivieren der Benutzerkontensteuerung definieren Sie können folgende Parameterwerte verwenden:
    - 0 – Gerät nie neu starten.
    - 1 – Gerät neu starten, wenn die Benutzerkontensteuerung vor dem Start des Tools aktiviert wurde.
    - 2 – Gerät zwingend neu starten, wenn die Benutzerkontensteuerung vor dem Start des Tools aktiviert wurde.
    - 4 – Gerät immer neu starten.
    - 5 – Gerät immer zwingend neu starten.
- Geben Sie im Abschnitt `UserAccount` den Namen des Benutzerkontos (`user`) und dessen Kennwort (`Pwd`) ein.

Beispiel für Inhalt einer Konfigurationsdatei:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

Nach Abschluss der Ausführung des Tools werden im Startordner die folgenden Dateien erstellt:

- riprep.txt – Bericht über den Verlauf, in dem die Vorgänge des Tools mit Beschreibungen angegeben sind.
- riprep.log – Protokolldatei (wird angelegt, wenn eine Ablaufverfolgungsstufe größer 0 eingegeben wurde).

Programme lokal installieren

In diesem Abschnitt wird der Installationsvorgang der Programme beschrieben, die nur lokal auf den Geräten installiert werden können.

Um eine lokale Installation von Programmen auf einem ausgewählten Client-Gerät durchzuführen, müssen Sie über Administratorrechte auf diesem Gerät verfügen.

► *Gehen Sie wie folgt vor, um Programme auf einem ausgewählten Client-Gerät lokal zu installieren:*

1. Installieren Sie auf dem Client-Gerät den Administrationsagenten, und passen Sie die Verbindung des Client-Geräts mit dem Administrationsserver an.
2. Installieren Sie die erforderlichen Programme auf dem Gerät. Folgen Sie dabei den Anweisungen in den Handbüchern zu diesen Programmen.
3. Installieren Sie auf dem Administrator-Arbeitsplatz das Verwaltungs-Plug-in für jedes installierte Programm.

Außerdem unterstützt Kaspersky Security Center die Möglichkeit zur lokalen Installation von Programmen mithilfe eines autonomen Installationspakets.

Autonome Installationspakete können für folgende Programme erstellt werden:

- Für Workstations:
  - Kaspersky Endpoint Security 10 für Windows (unterstützt alle Versionen)
  - Kaspersky Endpoint Security 10 für Linux (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)
  - Kaspersky Endpoint Security 8 für Linux (unterstützt alle Versionen)
  - Kaspersky Endpoint Security 10 für Mac (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)

- Kaspersky Endpoint Security 8 for Mac (unterstützt alle Versionen)
- Kaspersky Embedded Systems Security für Windows (geplante Veröffentlichung im November 2016).

- Für mobile Geräte:
  - Kaspersky Security 10 für mobile Endgeräte (Installation bei Aktivierung der Funktion Mobile Geräte verwalten verfügbar).

- Für E-Mailsysteme und Server for Collaboration
  - Kaspersky Security 8.0 für Linux Mail Server Maintenance Pack 1 (und höher)
  - Kaspersky Secure Mail Gateway 1.0
  - Kaspersky Security für Microsoft Exchange Server (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)
  - Kaspersky Security für SharePoint Server (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)

- Für Dateiserver:
  - Kaspersky Endpoint Security 10 für Windows (unterstützt alle Versionen)
  - Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition (unterstützt alle Versionen)
  - Kaspersky Security 10 für Windows Server (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)
  - Kaspersky Anti-Virus 8.0 für Linux File Server (unterstützt alle Versionen)
  - Kaspersky Anti-Virus 10 für Linux File Server (geplante Veröffentlichung in der zweiten Hälfte des Jahres 2016)

- Für virtuelle Maschinen:
  - Kaspersky Security für Virtualisierung 3.0 Agentless
  - Kaspersky Security für Virtualisierung 4.0 Agentless (geplante Veröffentlichung im November 2016)
  - Kaspersky Security für Virtualisierung 3.0 Light Agent (unterstützt alle Versionen)
  - Kaspersky Security für Virtualisierung 4.0 Light Agent (geplante Veröffentlichung im November 2016).
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Networks
  - Kaspersky Industrial Cyber Security for Nodes.

Informationen über die neuesten Programmversionen erhalten Sie auf der Website des Technischen Supports auf der Seite von Kaspersky Security Center 10, im Abschnitt Allgemeine Infos (http://support.kaspersky.com/de/12029).

In diesem Abschnitt

Lokale Installation des Administrationsagenten

► *Um den Administrationsagenten lokal auf einem Gerät zu installieren, gehen Sie wie folgt vor:*

1. Führen Sie auf dem Gerät die Datei setup.exe von der Distributions-CD oder der Distribution, die Sie aus dem Internet heruntergeladen haben, aus.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

2. Starten Sie im Fenster mit der Programmauswahl über den Link **Nur Administrationsagent für Kaspersky Security Center installieren** den Installationsassistenten des Administrationsagenten. Folgen Sie den Anweisungen des Assistenten.

   Bei der Ausführung des Installationsassistenten können Sie die erweiterten Einstellungen des Administrationsagenten anpassen (s. unten). Der Installationsvorgang des Administrationsagenten von dem aus dem Internet heruntergeladenen Archiv stimmt mit dem Installationsvorgang des Administrationsagenten von CD-ROM überein.

3. Soll ein Gerät als Verbindungs-Gateway für eine gewählte Administrationsgruppe verwendet werden, wählen Sie im Fenster **Verbindungs-Gateway** des Assistenten die Option **Als Verbindungs-Gateway in der demilitarisierten Zone verwenden**.

4. Um den Administrationsagenten bei der Installation auf der virtuellen Maschine anzupassen, gehen Sie wie folgt vor:

   a. Aktivieren Sie den dynamischen Modus für den Administrationsagenten für Virtual Desktop Infrastructure (VDI). Aktivieren Sie dazu im Fenster **Erweiterte Einstellungen** des Installationsassistenten das Kontrollkästchen **Dynamischen Modus für VDI aktivieren**.

   b. Optimieren Sie die Arbeit des Administrationsagenten für die virtuelle Infrastruktur. Aktivieren Sie dazu im Fenster **Erweiterte Einstellungen** des Installationsassistenten das Kontrollkästchen **Einstellungen des Kaspersky Security Center Administrationsagenten für die virtuelle Infrastruktur optimieren**.

Daraufhin wird die Prüfung der ausführbaren Dateien auf Schwachstellen beim Start des Geräts deaktiviert. Außerdem wird die Übertragung folgender Informationen auf den Administrationsserver deaktiviert:

- über die Hardwareinventur
- Auf dem Gerät installierten Programme
- über die Microsoft Windows-Updates, die auf dem lokalen Client-Gerät installiert werden sollen
- über die auf dem lokalen Client-Gerät gefundenen Software-Schwachstellen

Im Folgenden können Sie die Übertragung dieser Informationen in den Eigenschaften des Administrationsagenten oder in den Einstellungen der Richtlinie des Administrationsagenten aktivieren.

Nach Abschluss des Installationsassistenten wird der Administrationsagent auf dem Gerät installiert.

Sie können sich die Eigenschaften des Dienstes des Kaspersky Security Center Administrationsagenten anzeigen lassen, den Administrationsagenten starten und beenden sowie seine Ausführung mit den Standard-Administrationswerkzeugen von Microsoft Windows (Computerverwaltung\Dienste) verfolgen.

Installation des Administrationsagenten im Silent-Modus

Der Administrationsagent kann im Silent-Modus installiert werden, d. h. ohne die interaktive Eingabe von Installationseinstellungen. Für die Silent-Installation dient das msi-Installationspaket für den Administrationsagenten, das sich im Programmpaket für Kaspersky Security Center im Ordner Packages\NetAgent\exec befindet.

► *Um den Administrationsagenten im Silent-Modus auf einem lokalen Gerät zu installieren,*

geben Sie folgenden Befehl ein:

```
msiexec /i "Kaspersky Network Agent.msi"
/qn <setup_parameters>
```

, wobei `setup_parameters` – Liste mit Einstellungen und Einstellungswerten, die durch Leerzeichen getrennt werden (`PRO1=PROP1VAL PROP2=PROP2VAL`).

Die Namen und die möglichen Einstellungswerte, die bei der Installation des Administrationsagenten im Silent-Modus zulässig sind, sind in folgender Tabelle angegeben.

Tabelle 8. Einstellungen für die Installation des Administrationsagenten im Silent-Modus

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
INSTALLDIR	Pfad des Installationsordners für den Administrationsagenten	Zeichenfolgenwert.
SERVERADDRESS	Adresse des Administrationsservers	Zeichenfolgenwert.
SERVERPORT	Portnummer für das Herstellen einer Verbindung mit dem Administrationsserver	Zahlenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
SERVERSSLPORT	Portnummer für das Herstellen einer sicheren Verbindung mit dem Administrationsserver über das SSL-Protokoll	Zahlenwert.
USESSL	Soll eine SSL-Verbindung verwendet werden?	• 1 – verwenden. • Anderer Wert oder keine Angabe – nicht verwenden.
OPENUDPPORT	Soll ein UDP-Port geöffnet werden?	• 1 – öffnen. • Anderer Wert oder keine Angabe – öffnen.
UDPPORT	UDP-Port	Zahlenwert.
USEPROXY	Soll ein Proxyserver verwendet werden?	• 1 – verwenden. • Anderer Wert oder keine Angabe – nicht verwenden.
PROXYADDRESS	Proxyserver Adresse	Zeichenfolgenwert.
PROXYPORT	Portnummer für die Verbindung mit dem Proxyserver	Zahlenwert.
PROXYLOGIN	Benutzerkonto-Name für die Verbindung mit dem Proxyserver	Zeichenfolgenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
PROXYPASSWORD	Kennwort des Benutzerkontos für die Verbindung mit dem Proxyserver. Geben Sie in den Einstellungen der Installationspakete die Daten der privilegierten Benutzerkonten nicht an.	Zeichenfolgenwert.
GATEWAYMODE	Modus für die Nutzung eines Verbindungs-Gateways	• 0 – Verbindungs-Gateway nicht verwenden. • 1 – Als Verbindungs-Gateway wird das Gerät verwendet, auf dem der Administrationsagent installiert ist. • 2 – Über ein anderes Verbindungs-Gateway mit dem Administrationsserver verbinden.
GATEWAYADDRESS	Adresse des Verbindungs-Gateways	Zeichenfolgenwert.
CERTSELECTION	Methode zum Anfordern eines Zertifikats	• GetOnFirstConnection – Zertifikat des Administrationsservers anfordern. • GetExistent – Vorhandenes Zertifikat auswählen.
CERTFILE	Pfad der Zertifikatsdatei	Zeichenfolgenwert.
VMVDI	Soll der dynamische VDI-Modus aktiviert werden?	• 1 – aktivieren. • Anderer Wert oder keine Angabe – nicht aktivieren.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
LAUNCHPROGRAM	Soll der Dienst des Administrationsagenten nach dem Abschluss der Installation gestartet werden?	• 1 – starten. • Anderer Wert oder keine Angabe – nicht starten.

Die Remote-Installation des Administrationsagenten mithilfe eines Installationspakets oder die lokale Installation im Silent-Modus setzt das Einverständnis mit den Bedingungen des Lizenzvertrags für das zu installierende Programm voraus. Der Endbenutzer-Lizenzvertrag für ein konkretes Programm ist im Lieferumfang des entsprechenden Programms enthalten oder kann auf der Webseite des Technischen Supports von Kaspersky Lab eingesehen werden.

Lokale Installation des Verwaltungs-Plug-ins für das Programm

► *Damit das Verwaltungs-Plug-in für das Programm installiert wird,*

starten Sie auf dem Gerät, auf dem die Verwaltungskonsole installiert ist, die ausführbare Datei klcfginst.exe, die zum Lieferumfang des Programms gehört.

Die Datei klcfginst.exe gehört zu allen Programmen, die über Kaspersky Security Center verwaltet werden. Die Installation wird von einem Assistenten begleitet und muss nicht konfiguriert werden.

Installation von Programmen im Silent-Modus

► *Um ein Programm im nicht interaktiven Modus zu installieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmhauptfenster von Kaspersky Security Center.
2. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur im Unterordner **Installationspakete** das Installationspaket für das gewünschte Programm aus oder erstellen Sie für dieses Programm ein neues Installationspaket.

   Das Installationspaket wird auf dem Administrationsserver im gemeinsamen Ordner im Dienstordner Packages gespeichert. Jedem Installationspaket entspricht dabei der jeweilige Unterordner.

3. Öffnen Sie den Ordner des gewünschten Installationspakets auf eine der folgenden Weisen:

   - Kopieren Sie den Ordner, der zum gewünschten Installationspaket passt, vom Administrationsserver auf das Client-Gerät. Öffnen Sie danach den kopierten Ordner auf dem Client-Gerät.
   - Öffnen Sie anschließend vom Client-Gerät aus den gemeinsamen Ordner auf dem Administrationsserver, der zum gewünschten Installationspaket passt.

   Wenn sich der freigegebene Ordner auf einem Gerät mit dem Betriebssystem Microsoft Windows Vista befindet, muss der Wert **Deaktiviert** für die Einstellung **Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen** (**Start** → **Systemsteuerung** → **Verwaltung** → **Lokale Sicherheitsrichtlinie** → **Sicherheitseinstellungen**) gewählt werden.

4. Je nach dem gewählten Programm gehen Sie wie folgt vor:

   - Bei Kaspersky Anti-Virus für Windows Workstation, Kaspersky Anti-Virus für Windows Server und Kaspersky Security Center wechseln Sie in den Unterordner exec und starten Sie die ausführbare Datei (mit der Endung .exe) mit dem Parameter /s.

   - Bei den übrigen Programmen von Kaspersky Lab starten Sie aus dem geöffneten Ordner die ausführbare Datei (mit der Erweiterung .exe) mit dem Schlüssel /s.

   Der Start einer ausführbaren Datei mit dem Schlüssel `EULA=1` bedeutet, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren. Der Text des Lizenzvertrags ist im Lieferumfang von Kaspersky Security Center enthalten. Die Annahme der Bedingungen des Lizenzvertrags ist die Voraussetzung für die Installation oder das Update des Programms.

Programme mithilfe autonomer Installationspakete installieren

Kaspersky Security Center ermöglicht das Erstellen von autonomen Installationspaketen für Programme. Bei einem autonomen Installationspaket handelt es sich um eine ausführbare Datei, die auf einem Webserver gestellt, per E-Mail verschickt oder auf andere Weise auf ein Client-Gerät übermittelt werden kann. Die empfangene Datei kann lokal auf dem Client-Gerät gestartet werden, um das Programm ohne Beteiligung von Kaspersky Security Center zu installieren.

► *Um ein Programm mithilfe des autonomen Installationspakets zu installieren, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.

2. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

3. Wählen Sie im Arbeitsplatz das Installationspaket für das gewünschte Programm aus.

4. Starten Sie den Vorgang zum Erstellen eines autonomen Installationspakets auf eine der folgenden Weisen:

- Klicken Sie mit der rechten Maustaste auf das Installationspaket und wählen **Autonomes Installationspaket anlegen** aus.
- Klicken Sie im Arbeitsbereich des Installationspakets auf den Link **Autonomes Installationspaket anlegen**.

Daraufhin wird der Assistent für das Erstellen von autonomen Installationspaketen gestartet. Folgen Sie den Anweisungen.

Wählen Sie im letzten Schritt des Assistenten eine Methode für die Übertragung des autonomen Installationspakets auf das Client-Gerät aus.

5. Übertragen Sie das autonome Installationspaket für das Programm auf das Client-Gerät.
6. Starten Sie das autonome Installationspaket auf dem Client-Gerät.

Daraufhin wird das Programm auf dem Client-Gerät mit den Einstellungen installiert, die im autonomen Paket vorgegeben wurden.

Beim Erstellen wird ein autonomes Installationspaket automatisch auf dem Webserver veröffentlicht. Der Link für den Download des autonomen Paketes wird in der Liste der erstellten autonomen Installationspakete angezeigt. Bei Bedarf können Sie die Veröffentlichung des gewählten autonomen Paketes abbrechen und es erneut auf dem Webserver veröffentlichen. Standardmäßig wird für den Download der autonomen Installationspakete Port 8060 verwendet.

Verteilung der Verwaltungssysteme für mobile Geräte

In diesem Abschnitt wird die Verteilung der Verwaltungssysteme für mobile Geräte mithilfe der Protokolle Exchange ActiveSync, iOS MDM und Kaspersky Endpoint Security beschrieben.

In diesem Abschnitt

Verwaltung mithilfe von iOS MDM- und Microsoft Exchange ActiveSync-Protokollen

In Kaspersky Security Center können Sie mobile Geräte verwalten, die über das Exchange ActiveSync-Protokoll mit dem Administrationsserver verbunden sind. Mobilgeräte, die mit dem Exchange ActiveSync-Server für mobile Geräte verbunden sind und vom Administrationsserver verwaltet werden, werden Exchange ActiveSync-Mobilgeräte (EAS-Geräte) genannt.

Das Exchange ActiveSync-Protokoll unterstützt folgende Betriebssysteme:

- Windows Mobile
- Windows CE
- Windows Phone® 7

- Windows Phone 8
- Android
- Bada
- BlackBerry® 10
- iOS®
- Symbian.

> Die Auswahl der Einstellungen für die Geräteverwaltung mithilfe von Exchange ActiveSync ist vom Betriebssystem abhängig, mit dem das mobile Gerät arbeitet.
> Einzelheiten zur Unterstützung des Exchange ActiveSync-Protokolls für ein konkretes Betriebssystem erhalten Sie in der Dokumentation des Betriebssystems.

Die Verteilung des Verwaltungssystems für mobile Geräte mithilfe des Exchange ActiveSync-Protokolls wird in der folgenden Reihenfolge durchgeführt:

1. Der Administrator installiert auf dem ausgewählten Client-Gerät den Exchange ActiveSync-Server für mobile Geräte (s. Abschnitt "Exchange ActiveSync-Server für mobile Geräte installieren" auf S. 151).
2. Der Administrator erstellt in der Verwaltungskonsole ein Profil (mehrere Profile) für die Verwaltung von EAS-Geräten und fügt dieses Profil zu den E-Mail-Postfächern der Exchange ActiveSync-Benutzer hinzu.

   > Bei einem *Profil zur Verwaltung von Exchange ActiveSync-Mobilgeräten* handelt es sich um eine ActiveSync-Richtlinie, die für die Verwaltung von Exchange ActiveSync-Mobilgeräten verwendet wird. Einem Microsoft Exchange-Postfach kann nur ein Verwaltungsprofil für EAS-Geräte zugewiesen werden.

   Eine Anleitung zur Erstellung eines Profils zur Verwaltung von EAS-Geräten finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

   Die Benutzer von mobilen EAS-Geräten stellen eine Verbindung zu ihren Exchange-Postfächern her. Das Verwaltungsprofil legt Beschränkungen für mobile Geräte fest (s. Abschnitt "Mobile Geräte mit dem Exchange ActiveSync-Server für mobile Geräte verbinden" auf S. 153).

Informationen zum Hinzufügen des Profils für die Verwaltung von EAS-Geräten und Exchange ActiveSync-Mobilgeräten finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

Exchange ActiveSync-Server für mobile Geräte installieren

Der Exchange ActiveSync-Server für mobile Geräte wird auf dem Client-Gerät installiert, auf dem sich der Microsoft Exchange-Server befindet. Es wird empfohlen, den Exchange ActiveSync-Server für mobile Geräte auf dem Microsoft Exchange-Server mit der Rolle Client Access zu installieren. Wurden in einer Domain mehrere Microsoft Exchange-Server mit der Rolle Client Access zu einem Array (Client Access Array) zusammengefasst, so wird empfohlen, den Exchange ActiveSync-Server für mobile Geräte im Cluster-Modus auf jedem Microsoft Exchange-Server des Arrays zu installieren.

► *Um einen Exchange ActiveSync-Server für mobile Geräte auf einem lokalen Gerät zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

2. Starten Sie im Fenster mit der Programmauswahl über den Link **Exchange ActiveSync-Server für mobile Geräte installieren** den Installationsassistenten für den Exchange ActiveSync-Server für mobile Geräte.

3. Wählen Sie im Fenster **Installationseinstellungen** einen Installationstyp für den Exchange ActiveSync-Server für mobile Geräte aus:

   - Wenn Sie den Exchange ActiveSync-Server für mobile Geräte mit den Standardeinstellungen installieren möchten, wählen Sie die Option **Standardinstallation** und klicken Sie auf **Weiter**.

   - Wenn Sie die Einstellungen für die Installation des Exchange ActiveSync-Server für mobile Geräte manuell anpassen möchten, wählen Sie die Variante **Erweiterte Installation** aus und klicken Sie auf **Weiter**. Gehen Sie anschließend wie folgt vor:

     a. Wählen Sie im Fenster **Zielordner** einen Zielordner aus. Standardmäßig ist es <Laufwerk>:\Programme\Kaspersky Lab\Mobile Device Management for Exchange. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** wechseln.

b. Wählen Sie im Fenster **Installationsmodus** einen Modus für die Installation des Exchange ActiveSync-Server für mobile Geräte aus: normaler Modus oder Cluster-Modus.

c. Wählen Sie im Fenster **Benutzerkonto wählen** ein Benutzerkonto aus, das für die Verwaltung von mobilen Geräten verwendet werden soll:

- **Benutzerkonto und Rollengruppe automatisch erstellen**.
  Das Benutzerkonto wird automatisch erstellt.
- **Benutzerkonto angeben**. Das Benutzerkonto muss manuell ausgewählt werden. Geben Sie mithilfe der Schaltfläche **Auswählen** einen Benutzer an, dessen Benutzerkonto verwendet wird, und legen Sie ein Kennwort fest. Der gewählte Benutzer soll zur Gruppe mit den Rechten für die Verwaltung von mobilen Geräten über ActiveSync gehören.

d. Erlauben oder verbieten Sie im Fenster **IIS-Einstellungen** die automatische Konfiguration der Einstellungen für den Webserver Internet Information Services (IIS).

> Wenn Sie die automatische Konfiguration der IIS-Einstellungen verboten haben, aktivieren Sie in den IIS-Einstellungen des virtuellen Verzeichnisses PowerShell manuell das Authentifizierungsverfahren "Windows Authentication". Wenn das Authentifizierungsverfahren "Windows Authentication" nicht aktiviert ist, funktioniert der Exchange ActiveSync-Server für mobile Geräte nicht. Informationen zur Funktion der IIS-Einstellungen finden Sie in der Dokumentation für diesen Webserver.

e. Klicken Sie auf die Schaltfläche **Weiter**.

4. Überprüfen Sie im folgenden Fenster die Einstellungen für die Installation des Exchange ActiveSync-Server für mobile Geräte und klicken Sie auf **Installieren**.

Nach Abschluss des Assistenten wird der Exchange ActiveSync-Server für mobile Geräte auf dem lokalen Gerät installiert. Der Exchange ActiveSync-Server für mobile Geräte wird im Ordner **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

Mobile Geräte mit dem Exchange ActiveSync-Server für mobile Geräte verbinden

Vor dem Verbinden der mobilen Geräte muss der Microsoft Exchange Server angepasst werden, um eine Verbindung der Geräte über das ActiveSync-Protokoll zu ermöglichen.

Um ein mobiles Gerät mit dem Exchange ActiveSync-Server für mobile Geräte zu verbinden, stellt der Benutzer eine Verbindung zu seinem Microsoft Exchange-Postfach mittels ActiveSync her. Beim Herstellen der Verbindung muss der Benutzer im ActiveSync-Client Verbindungseinstellungen angeben, beispielsweise, E-Mail-Adresse und das Kennwort für das E-Mail-Konto.

Das mobile Gerät des Benutzers, das mit dem Microsoft Exchange-Server verbunden ist, wird im Unterordner **Mobile Geräte** angezeigt, der sich im Ordner **Mobile Geräte verwalten** der Konsolenstruktur befindet.

Nach dem Verbindungsaufbau zwischen dem Exchange ActiveSync-Mobilgerät und dem Exchange ActiveSync-Server für mobile Geräte kann der Administrator das angeschlossene Exchange ActiveSync-Mobilgerät verwalten. Informationen zur Verwaltung von Exchange ActiveSync-Mobilgeräten können Sie dem *Kaspersky Security Center Administratorhandbuch* entnehmen.

Verteilung des Verwaltungssystems mithilfe des iOS MDM-Protokolls

Kaspersky Security Center ermöglicht die Verwaltung von mobilen Geräten auf der iOS-Plattform. Mobile iOS-Geräte, die mit dem iOS MDM-Server verbunden sind und vom Administrationsserver verwaltet werden, werden mobile iOS MDM-Geräte genannt.

Mobile Geräte werden folgendermaßen mit dem iOS MDM-Server verbunden:

1. Der Administrator installiert den iOS MDM-Server auf einem ausgewählten Client-Gerät. Die Installation des iOS MDM-Servers erfolgt mit den normalen Tools des Betriebssystems.

2. Der Administrator fordert ein Zertifikat des Typs Apple® Push Notification Service (APNs-Zertifikat) an (s. Abschnitt "APNs-Zertifikat anfordern" auf S. 163).

   Ein APNs-Zertifikat ermöglicht dem Administrationsserver eine Verbindung zum APNs-Server, um Push-Benachrichtigungen an mobile iOS MDM-Geräte zu schicken.

3. Der Administrator installiert das APNs-Zertifikat auf dem iOS MDM-Server (s. Abschnitt "APNs-Zertifikat auf dem iOS MDM-Server installieren" auf S. 165).

4. Der Administrator erstellt ein iOS MDM-Profil für den Benutzer des mobilen iOS-Geräts.

   Das iOS MDM-Profil enthält eine Auswahl von Einstellungen für die Verbindung von mobilen iOS-Geräten zum Administrationsserver.

5. Der Administrator stellt für den Benutzer ein allgemeines Zertifikat aus (s. Abschnitt "Allgemeines Zertifikat ausstellen und auf dem mobilen Gerät installieren" auf S. 166).

   Das allgemeine Zertifikat dient als Beweis, dass das mobile Gerät dem Benutzer gehört.

6. Der Benutzer folgt dem Link, den er vom Administrator erhalten hat, und lädt das Installationspaket auf das mobile Gerät herunter.

   Das Installationspaket enthält das Zertifikat und das iOS MDM-Profil.

   Nach dem Download des iOS MDM-Profils und der Synchronisierung mit dem Administrationsserver wird das iOS MDM-Mobilgerät im Ordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

7. Der Administrator fügt das Konfigurationsprofil auf dem iOS MDM-Server hinzu und installiert es auf dem mobilen Gerät, sobald dieses verbunden wird.

   Das Konfigurationsprofil enthält eine Auswahl von Einstellungen und Einschränkungen für mobile Geräte mit iOS MDM. Dazu zählen beispielsweise Einstellungen für die Installation von Apps und für die Verwendung bestimmter Funktionen von mobilen

Geräten sowie Einstellungen für die Nutzung von E-Mail und Kalender. Mithilfe eines Konfigurationsprofils können mobile iOS MDM-Geräte gemäß den Sicherheitsrichtlinien eines Unternehmens angepasst werden.

8. Bei Bedarf fügt der Administrator auf dem iOS MDM-Server Provisioning-Profile hinzu und installiert diese anschließend auf mobilen Geräten.

   Bei einem *Provisioning-Profil* handelt es sich um ein Profil, das zur Verwaltung von Anwendungen verwendet wird, die sich nicht über einen App Store® vertreiben lassen. Ein Provisioning-Profil enthält Informationen zur Lizenz und ist mit einer bestimmten App verbunden.

Informationen zur Verwaltung von mobilen iOS MDM-Geräten können Sie dem *Kaspersky Security Center Administratorhandbuch* entnehmen.

In diesem Abschnitt

iOS MDM-Server installieren

► *Um einen iOS MDM-Server auf einem lokalen Gerät zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die ausführbare Datei setup.exe.

   Ein Fenster wird geöffnet, in dem Sie Programme von Kaspersky Lab zur Installation auswählen können.

   Starten Sie im Fenster mit der Programmauswahl über den Link **iOS MDM-Server installieren** den Installationsassistenten für den iOS MDM-Server.

2. Wählen Sie den Zielordner aus.

   Standardmäßig ist es <Laufwerk>:\Programme\Kaspersky Lab\Mobile Device Management for iOS. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch bei der Installation angelegt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.

3. Geben Sie im Assistentenfenster **Einstellungen für die Verbindung mit dem iOS MDM-Server** im Feld **Externer Port zur Verbindung mit dem iOS MDM-Dienst** einen externen Port für die Verbindung von mobilen Geräten mit dem iOS MDM-Dienst an.

   Der externe Port 5223 wird durch mobile Geräte für die Verbindung mit dem APNs-Server verwendet. Stellen Sie sicher, dass der Port 5223 in der Firewall für die Verbindung mit dem Adressbereich 17.0.0.0/8 geöffnet ist.

   Für die Verbindung des Geräts mit dem iOS MDM-Server wird standardmäßig der Port 443 verwendet. Wenn der Port 443 schon von einem anderen Dienst oder einer anderen App verwendet wird, kann er, beispielsweise, auf den Port 9443 geändert werden.

   Der iOS MDM-Server verwendet den externen Port 2195 zum Senden von Benachrichtigungen an den APNs-Server.

Die APNs-Server werden im Modus der ausgeglichenen Auslastung ausgeführt. Die mobilen Geräte verbinden sich nicht immer mit denselben IP-Adressen, um Benachrichtigungen zu erhalten. Der Adressbereich 17.0.0.0/8 ist Apple zugeordnet, daher wird empfohlen, den gesamten Bereich in den Einstellungen der Firewall als erlaubt anzugeben.

4. Wenn Sie die Interaktionsports für die Programmkomponenten manuell anpassen möchten, aktivieren Sie das Kontrollkästchen **Lokale Ports manuell anpassen** und nehmen Sie dann folgende Einstellungen vor:

   - **Port zur Verbindung mit dem Administrationsagenten**. Geben Sie in diesem Feld den Port für die Verbindung des iOS MDM-Dienstes mit dem Administrationsagenten. Standardmäßig wird Port 9799 verwendet.

   - **Port für die Verbindung mit dem iOS MDM-Dienst**. Geben Sie in diesem Feld den lokalen Port für die Verbindung des Administrationsagenten mit dem iOS MDM-Dienst an. Standardmäßig wird Port 9899 verwendet.

   Es wird empfohlen, die Standardeinstellungen zu verwenden.

5. Geben Sie im Assistentenfenster **Externe Adresse des Servers für mobile Geräte** im Feld **Webadresse für Remoteverbindung mit dem Server für mobile Geräte** die Adresse des Client-Geräts an, auf dem der iOS MDM-Server installiert wird.

   Diese Adresse wird für die Verbindung von verwalteten mobilen Geräten zum iOS MDM-Dienst verwendet. Das Client-Gerät muss für eine Verbindung von iOS MDM-Geräten verfügbar sein.

   Sie können die Adresse des Client-Geräts in einem der folgenden Formate angeben:

   - FQDN-Name des Geräts (Beispiel: mdm.example.com)

   - NetBIOS-Name des Geräts

   - IP-Adresse des Geräts.

Bitte fügen Sie das URL-Schema und die Portnummer in die Adresszeile nicht ein. Diese Werte werden automatisch gesetzt.

Der Assistent installiert den iOS MDM-Server auf dem lokalen Gerät. Der iOS MDM-Server wird im Ordner **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

iOS MDM-Server im Silent-Modus installieren

Kaspersky Security Center erlaubt die Installation des iOS MDM-Servers auf dem lokalen Gerät im Silent-Modus. d. h. ohne interaktive Eingabe der Installationseinstellungen.

► *Um einen iOS MDM-Server auf einem lokalen Gerät im Silent-Modus zu installieren,*

geben Sie folgenden Befehl ein:

```
.\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1
<setup_parameters>"
```

wobei `setup_parameters` eine Aufzählung von Einstellungen und Einstellungswerten ist, die durch Leerzeichen getrennt werden (`PRO1=PROP1VAL PROP2=PROP2VAL`).
Die Datei setup.exe, die sich auf der CD-ROM des Programms Kaspersky Security Center im Ordner Server befindet.

Die Namen und die möglichen Einstellungswerte, die bei der Installation des iOS MDM-Servers im Silent-Modus zulässig sind, werden in folgender Tabelle angegeben. Die Einstellungen können in beliebiger Reihenfolge angegeben werden.

Tabelle 9. Einstellungen für die Installation des iOS MDM-Servers im Silent-Modus

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags. Dieser Einstellung ist verpflichtend.	• 1 – Die Bedingungen des Lizenzvertrags werden akzeptiert. • Anderer Wert oder keine Angabe – die Bedingungen des Endbenutzer-Lizenzvertrags werden abgelehnt (die Installation wird nicht ausgeführt).
DONT_USE_ANSWER_FILE	xml-Datei mit den Installationseinstellungen des iOS MDM-Servers verwenden oder nicht. Die xml-Datei ist Teil des Lieferumfangs des Installationspakets oder befindet sich auf dem Administrationsserver. Der Pfad der Datei muss nicht zusätzlich angegeben werden. Dieser Einstellung ist verpflichtend.	• 1 – xml-Datei mit den Einstellungen nicht verwenden. • Anderer Wert oder keine Angabe – xml-Datei mit den Einstellungen verwenden.
INSTALLDIR	Installationsordner des iOS MDM-Servers. Dieser Einstellung ist nicht verpflichtend.	Zeichenfolgenwert, beispielsweise `INSTALLDIR=\"C:\install\"`

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
CONNECTORPORT	Lokaler Port für die Verbindung des iOS MDM-Dienstes mit dem Administrations-agenten. Standardmäßig wird Port 9799 verwendet. Dieser Einstellung ist nicht verpflichtend.	Zahlenwert.
LOCALSERVERPORT	Lokaler Port für die Verbindung des Administrationsagenten mit dem iOS MDM-Dienst. Standardmäßig wird Port 9899 verwendet. Dieser Einstellung ist nicht verpflichtend.	Zahlenwert.
EXTERNALSERVERPORT	Port für die Verbindung des Geräts mit dem iOS MDM-Server. Standardmäßig wird Port 443 verwendet. Dieser Einstellung ist nicht verpflichtend.	Zahlenwert.

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
EXTERNAL_SERVER_URL	Externe Adresse des Client-Geräts, auf dem der iOS MDM-Server installiert wird. Diese Adresse wird für die Verbindung von verwalteten mobilen Geräten zum iOS MDM-Dienst verwendet. Das Client-Gerät muss für die Verbindung zu iOS MDM verfügbar sein. Die Adresse darf kein URL-Schema und keine Portnummer enthalten, diese Werte werden automatisch hinzugefügt. Dieser Einstellung ist nicht verpflichtend.	• FQDN-Name des Geräts (Beispiel: mdm.example.com). • NetBIOS-Name des Geräts. • IP-Adresse des Geräts.
WORKFOLDER	Arbeitsordner des iOS MDM-Servers. Wenn kein Arbeitsordner angegeben ist, werden die Daten in den Standardordner geschrieben. Dieser Einstellung ist nicht verpflichtend.	Zeichenfolgenwert, beispielsweise `WORKFOLDER=\"C:\work\"`

Name des Parameters	Beschreibung des Parameters	Mögliche Werte
MTNCY	iOS MDM-Server mit mehreren virtuellen Servern verwenden. Dieser Einstellung ist nicht verpflichtend.	• 1 – Der iOS MDM-Server wird von mehreren virtuellen Administrationsservern verwendet. • Anderer Wert oder keine Angabe – Der iOS MDM-Server wird nicht von mehreren virtuellen Administrationsservern verwendet.

Beispiel:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Die Installationseinstellungen des iOS MDM-Servers werden im Abschnitt iOS MDM-Server installieren (auf S. 155) im Detail beschrieben.

iOS MDM-Server mit mehreren virtuellen Servern verwenden

► *Um die Verwendung des iOS MDM-Servers durch mehrere virtuelle Administrationsserver zu aktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie die Systemregistrierung des Client-Geräts, auf dem der iOS MDM-Server installiert ist, z. B. lokal mit dem Befehl regedit im Menü **Start** → **Ausführen**.

2. Rufen Sie den folgenden Abschnitt auf:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0

3. Für den Schlüssel ConnectorFlags (DWORD) ist der Wert 02102482 festgelegt.

4. Rufen Sie den folgenden Abschnitt auf:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0

5. Für den Schlüssel ConnInstalled (DWORD) ist der Wert 00000001 festgelegt.

6. Dienst des iOS MDM-Servers neu starten.

Die Werte der Schlüssel müssen in der angegebenen Reihenfolge eingegeben werden.

APNs-Zertifikat anfordern

Nachdem ein Certificate Signing Request (im Folgenden "CSR-Anfrage" genannt) erstellt wurde, wird beim ersten Schritt des Assistenten zum Anfordern eines APNs-Zertifikats der private Bestandteil des neuen Zertifikats (privater Schlüssel) im Arbeitsspeicher des Geräts gespeichert. Deshalb müssen alle Schritte des Assistenten innerhalb einer einzigen Programmsitzung abgeschlossen werden.

► *Um ein APNs-Zertifikat anzufordern, gehen Sie wie folgt vor:*

1. Wählen Sie im Ordner **Mobile Geräte** der Konsolenstruktur den iOS MDM-Server aus.

   Der Ordner **Mobile Geräte** befindet sich standardmäßig im Ordner **Erweitert**.

2. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen **Eigenschaften** aus.

   Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Zertifikate** aus.

4. Klicken Sie im Abschnitt **Zertifikate** im Einstellungsbereich **Apple Push Notification-Zertifikat** auf die Schaltfläche **Zertifikat anfordern**.

   Der Assistent zum Anfordern eines APNs-Zertifikats wird gestartet und das Fenster **Zertifikat anfordern** geöffnet.

5. Erstellen Sie einen Certificate Signing Request (im Folgenden "CSR-Anfrage" genannt). Gehen Sie dazu folgendermaßen vor:

    a. Klicken Sie auf **CSR erstellen**.

    b. Machen Sie im folgenden Fenster **CSR erstellen** folgende Angaben: Name der Anfrage, Name des Unternehmens und der Abteilung, Stadt, Bundesland und Land.

    c. Klicken Sie auf **Speichern** und geben Sie den Namen der Datei an, in der die CSR-Anfrage gespeichert werden soll.

    Der private Bestandteil (privater Schlüssel) des zu erstellenden Zertifikats wird im Arbeitsspeicher des Geräts abgelegt.

6. Senden Sie die erstellte Datei über Ihr CompanyAccount mit einer CSR-Anfrage auf Signatur an Kaspersky Lab.

    > Das Signieren einer CSR-Anfrage ist erst möglich, nachdem ein Schlüssel auf das Portal CompanyAccount hochgeladen wurde, der zur Nutzung der Funktionalität "Mobile Geräte verwalten" berechtigt.

    Nachdem Ihre Online-Anfrage bearbeitet wurde, erhalten Sie eine von Kaspersky Lab signierte Datei mit der CSR-Anfrage.

7. Senden Sie die signierte Datei mit der CSR-Anfrage an die Webseite von Apple Inc https://identity.apple.com/pushcert. Verwenden Sie dazu Ihre Apple-ID.

    > Die Verwendung einer persönlichen Apple ID wird nicht empfohlen. Erstellen Sie eine separate Apple-ID für die unternehmensbezogene Verwendung. Ordnen Sie die erstellte Apple-ID nicht dem E-Mail-Postfach eines einzelnen Mitarbeiters, sondern dem Postfach des Unternehmens zu.

    Nachdem die CSR-Anfrage von der Apple Inc. bearbeitet wurde, erhalten Sie den öffentlichen Bestandteil des APNs-Zertifikats. Speichern Sie diese Datei auf der Festplatte.

8. Exportieren Sie das APNs-Zertifikat zusammen mit dem privaten Schlüssel, der beim Erstellen der CSR-Anfrage generiert wurde, in eine PFX-Datei. Gehen Sie dazu folgendermaßen vor:

    a. Klicken Sie im Fenster **Neues APNs-Zertifikat anfordern** auf **CSR abschließen**.

    b. Wählen Sie im folgenden Fenster **Öffnen** die Datei mit dem öffentlichen Bestandteil des Zertifikats aus, die Sie nach der Bearbeitung der CSR-Anfrage von der Apple Inc erhalten haben, und klicken Sie auf **Öffnen**.

    Der Export des Zertifikats wird gestartet.

    c. Geben Sie im folgenden Fenster ein Kennwort für den privaten Schlüssel an und klicken Sie auf **OK**.

    Das Kennwort wird für die Installation des APNs-Zertifikats auf dem iOS MDM-Server verwendet.

    d. Geben Sie im folgenden Fenster **APNs-Zertifikat speichern** einen Namen für die Datei an, in der das APNs-Zertifikat gespeichert werden soll, wählen einen Ordner zum Speichern der Datei aus, und klicken Sie auf **Speichern**.

Der private und der öffentliche Bestandteil des Zertifikats werden kombiniert. Das APNs-Zertifikat wird in einer PFX-Datei gespeichert. Danach können Sie das APNs-Zertifikat auf dem iOS MDM-Server installieren (s. Abschnitt "APNs-Zertifikat auf dem iOS MDM-Server installieren" auf S. 165).

Einzelheiten darüber, wie eine Datei mit einer CSR-Anfrage erstellt und an Apple Inc. gesendet wird, finden Sie in der Wissensdatenbank auf der Webseite des Technischen Supports von Kaspersky Lab http://support.kaspersky.com/de/11077.

APNs-Zertifikat auf dem iOS MDM-Server installieren

Anschließend muss das APNs-Zertifikat auf dem iOS MDM-Server installiert werden.

► *Um ein APNs-Zertifikat auf dem iOS MDM-Server zu installieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Ordner **Mobile Geräte** der Konsolenstruktur den iOS MDM-Server aus.

   Der Ordner **Mobile Geräte** befindet sich standardmäßig im Ordner **Erweitert**.

2. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen **Eigenschaften** aus.

   Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Zertifikate** aus.

Klicken Sie im Abschnitt **Zertifikate** im Einstellungsbereich **Apple Push Notification-Zertifikat** auf die Schaltfläche **Installieren**.

1. Wählen Sie die PFX-Datei aus, die das APNs-Zertifikat enthält.

2. Geben Sie das Kennwort des privaten Schlüssels an, das beim Exportieren des APNs-Zertifikats festgelegt wurde (s. Abschnitt "APNs-Zertifikat anfordern" auf S. 163).

Das APNs-Zertifikat wird auf dem iOS MDM-Server installiert. Informationen über das Zertifikat werden im Eigenschaftenfenster des iOS MDM-Servers unter **Zertifikate** angezeigt.

Allgemeines Zertifikat ausstellen und auf dem mobilen Gerät installieren

► *Um ein allgemeines Zertifikat für den Benutzer auszustellen, gehen Sie folgendermaßen vor:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** ein Benutzerkonto aus.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Zertifikat installieren** aus.

   Der Assistent zur Zertifikatinstallation wird gestartet. Folgen Sie den Anweisungen.

Nach Abschluss des Assistenten wird ein Zertifikat erstellt und zur Liste der Benutzerzertifikate hinzugefügt.

Der Benutzer lädt das ausgestellte Zertifikat gemeinsam mit dem Installationspaket herunter, in dem sich das iOS MDM-Profil befindet.

Nachdem das mobile Gerät mit dem iOS MDM-Server verbunden wurde, werden auf dem Benutzergerät die Einstellungen des iOS MDM-Profils angewendet. Der Administrator kann verbundene Geräte verwalten.

Das mobile Gerät des Benutzers, das mit dem iOS MDM-Server verbunden ist, wird im Unterordner **Mobile Geräte** angezeigt, der sich im Ordner **Mobile Geräte verwalten** der Konsolenstruktur befindet.

Details über die Ausstellung von Zertifikaten und zur Verwaltung von mobilen iOS MDM-Geräten finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

iOS MDM-Gerät zur Liste der verwalteten Geräte hinzufügen

► *Um ein iOS MDM-Gerät des Benutzers mithilfe eines Links zum App Store zur Liste der verwalteten Geräte hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.

   Standardmäßig befindet sich der Ordner **Benutzerkonten** im Ordner **Erweitert**.

2. Wählen Sie das Benutzerkonto, dessen mobiles Gerät Sie zur Liste der verwalteten Geräte hinzufügen möchten.

3. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Gerät hinzufügen** aus.

   Der Assistent für das Hinzufügen von Geräten wird gestartet. Im Fenster **Quelle des Zertifikats** des Assistenten muss die Methode zur Erstellung des allgemeinen Zertifikats angegeben werden, mit dessen Hilfe der Administrationsserver das mobile Gerät identifiziert. Sie können ein allgemeines Zertifikat auf eine von zwei Arten angeben:

   - Automatisch ein allgemeines Zertifikat mithilfe des Administrationsservers erstellen und das Zertifikat auf dem Gerät hinzufügen.
   - Die Datei des allgemeinen Zertifikats angeben.

4. Wählen Sie im Fenster **Gerätetyp** des Assistenten die Variante **Link zum App Store**.

5. Konfigurieren Sie im Fenster **Benachrichtigungsmethode** des Assistenten die Benachrichtigungseinstellungen für den Benutzer des mobilen Geräts für die Benachrichtigung über die Erstellung eines Zertifikats (per SMS-Nachricht oder E-Mail).

6. Klicken Sie im Fenster **Informationen zum Zertifikat** auf die Schaltfläche **Fertig**, um den Assistent zum Erstellen eines neuen Zertifikats zu beenden.

Daraufhin werden ein Link und ein QR-Code zum Herunterladen von Kaspersky Safe Browser vom App Store an das Gerät des Benutzers gesendet. Der Benutzer klickt auf den Link oder scannt den QR-Code. Daraufhin zeigt das Betriebssystem dem Benutzer eine Zustimmungsaufforderung zur Installation von Kaspersky Safe Browser an. Der Benutzer

installiert Kaspersky Safe Browser auf dem mobilen Gerät. Nach der Installation von Kaspersky Safe Browser scannt der Benutzer nochmals den QR-Code zum Abrufen der Verbindungseinstellungen zum Administrationsserver. Nach dem erneuten Scannen des QR-Codes im Safe Browser erhält der Benutzer die Verbindungseinstellungen zum Administrationsserver und ein allgemeines Zertifikat. Das mobile Gerät stellt eine Verbindung zum Administrationsserver her und lädt ein allgemeines Zertifikat herunter.
Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

Wenn Kaspersky Safe Browser schon früher auf dem mobilen Gerät installiert wurde, müssen die Verbindungseinstellungen für den Administrationsserver selbstständig eingegeben werden. Der Benutzer scannt den QR-Code mithilfe der Scan-Funktion der App Kaspersky Safe Browser und erhält die Verbindungseinstellungen für die Verbindung des Geräts mit dem Administrationsserver. Die erhaltenen Einstellungen müssen vom Benutzer auf dem Gerät gespeichert werden. Im Weiteren stellt das mobile Gerät automatisch eine Verbindung zum Administrationsserver her und lädt ein allgemeines Zertifikat herunter. Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt. In diesem Fall wird Kaspersky Safe Browser nicht nochmals heruntergeladen und installiert.

Wenn auf dem iOS MDM-Gerät bereits früher ein iOS MDM-Profil installiert wurde, wird dieses Gerät nach der Installation von Kaspersky Safe Browser und des allgemeinen Zertifikats auf dem Gerät in der Geräteliste im Ordner **Mobile Geräte** zweimal angezeigt (dupliziert). Die Duplizierung in der Liste erfolgt aufgrund des Vorhandenseins von zwei allgemeinen (Identifikations-) Zertifikaten auf dem Gerät.

Verteilung des Verwaltungssystems mithilfe des KES-Protokolls und des Self Service Portals

Kaspersky Security Center ermöglicht den Benutzern, ihre über das KES-Protokoll mit dem Administrationsserver verbundenen mobilen Geräte mithilfe des Self Service Portals selbstständig zu verwalten.

> Das Self Service Portal unterstützt mobile Geräte mit den Betriebssystemen iOS und Android.

Die Verteilung des Verwaltungssystems mithilfe des KES-Protokolls und des Self Service Portals besteht aus folgenden Schritten:

1. Installation des Self Service Portals vorbereiten:

    a. Der Administrator installiert auf dem ausgewählten Client-Gerät das Self Service Portal (s. Abschnitt "Self Service Portal installieren" auf S. 173).

    b. Der Administrator gibt dem Benutzer die Adresse des Self Service Portals bekannt.

2. Mobiles Gerät mit dem Self Service Portal verbinden:

    a. Der Benutzer öffnet die Hauptseite des Portals.

    Das Self Service Portal erstellt ein Installationspaket und zeigt danach auf der Seite des Portals einen Einmallink zum Download des Pakets und einen QR-Code an, in dem der Link verschlüsselt ist. Das Installationspaket ist für die Installation des Verwaltungsagenten auf dem Gerät und die Anwendung der Unternehmensrichtlinien erforderlich.

    b. Der Benutzer wechselt mit dem mobilen Gerät, das zum Self Service Portal hinzugefügt werden soll, zur Downloadseite des Installationspakets, lädt das Installationspaket herunter und installiert den Verwaltungsagenten auf dem mobilen Gerät.

    c. Nach der Installation des Verwaltungsagenten wird das Gerät mit dem Administrationsserver verbunden.

Daraufhin wird das Gerät zur Liste der verwalteten Geräte hinzugefügt, und die Unternehmensrichtlinien werden auf das Gerät angewendet. Der Link mit Informationen über die Verbindung zum Administrationsserver wird dem Benutzer per E-Mail zugestellt.

Informationen zum Hinzufügen eines Geräts zum Self Service Portal finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

KES-Gerät zur Liste der verwalteten Geräte hinzufügen

► *Um ein KES-Gerät des Benutzers mithilfe eines Links zu Google Play™ zur Liste der verwalteten Geräte hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.

   Standardmäßig befindet sich der Ordner **Benutzerkonten** im Ordner **Erweitert**.

2. Wählen Sie das Benutzerkonto, dessen mobiles Gerät Sie zur Liste der verwalteten Geräte hinzufügen möchten.

3. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Gerät hinzufügen** aus.

   Der Assistent für das Hinzufügen von Geräten wird gestartet. Im Fenster **Quelle des Zertifikats** des Assistenten muss die Methode zur Erstellung des allgemeinen Zertifikats angegeben werden, mit dessen Hilfe der Administrationsserver das mobile Gerät identifiziert. Sie können ein allgemeines Zertifikat auf eine von zwei Arten angeben:

   - Automatisch ein allgemeines Zertifikat mithilfe des Administrationsservers erstellen und das Zertifikat auf dem Gerät hinzufügen.
   - Die Datei des allgemeinen Zertifikats angeben.

4. Wählen Sie im Fenster **Gerätetyp** des Assistenten die Variante **Link zu Google Play**.

5. Konfigurieren Sie im Fenster **Benachrichtigungsmethode** des Assistenten die Benachrichtigungseinstellungen für den Benutzer des mobilen Geräts für die Benachrichtigung über die Erstellung eines Zertifikats (mithilfe einer SMS-Nachricht, per E-Mail oder durch Anzeige der Information nach Beendigung des Assistenten).

6. Klicken Sie im Fenster **Informationen zum Zertifikat** auf die Schaltfläche **Fertig**, um den Assistent zum Erstellen eines neuen Zertifikats zu beenden.

Daraufhin werden ein Link und ein QR-Code zum Herunterladen von Kaspersky Endpoint Security für Android von Google Play an das Gerät des Benutzers gesendet. Der Benutzer wechselt mithilfe des Links oder durch Scannen des QR-Codes zum App Store Google Play. Daraufhin zeigt das Betriebssystem dem Benutzer eine Zustimmungsaufforderung zur Installation von Kaspersky Endpoint Security für Android an. Nach dem Herunterladen und der Installation von Kaspersky Endpoint Security für Android stellt das mobile Gerät eine Verbindung zum Administrationsserver her und lädt das allgemeine Zertifikat herunter. Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

> Wenn die App Kaspersky Endpoint Security für Android bereits auf dem Gerät installiert ist, muss der Benutzer die vom Administrator erhaltenen Verbindungseinstellungen für den Administrationsserver selbstständig eingeben. Nach der Konfiguration der Verbindungseinstellungen stellt das mobile Gerät eine Verbindung mit dem Administrationsserver her. Der Administrator stellt ein allgemeines Zertifikat für das Gerät aus und sendet dem Benutzer eine E-Mail-Nachricht oder eine SMS mit dem Benutzernamen und dem Kennwort zum Herunterladen des Zertifikats. Der Benutzer lädt das allgemeine Zertifikat herunter und installiert es auf seinem Gerät.
> Nach der Installation des Zertifikats auf dem mobilen Gerät wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt. In diesem Fall wird Kaspersky Endpoint Security für Android nicht nochmals heruntergeladen und installiert.

Self Service Portal installieren

In diesem Abschnitt werden die Installationsvorbereitungen für das Self Service Portal sowie die einzelnen Installationsschritte beschrieben.

Das Gerät, auf dem das Self Service Portal verteilt werden soll, muss folgenden Anforderungen entsprechen:

- Auf dem Gerät muss der Administrationsserver installiert sein (s. Abschnitt "Bereitstellung des Administrationsservers" auf S. 50).
- Auf dem Gerät muss der iOS MDM-Server installiert sein (s. Abschnitt "Verteilung des Verwaltungssystems mithilfe des iOS MDM-Protokolls" auf S. 153).

Zur Installation des Self Service Portals werden die Rechte des lokalen Administrators auf dem Gerät verwendet, auf dem die Installation ausgeführt werden soll.

► *Um Self Service Portal auf dem lokalen Gerät zu installieren, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner "Self Service Portal" aus dem Ordner **Mobile Geräte verwalten** aus.
2. Klicken Sie im Arbeitsplatz des Ordners auf die Schaltfläche **Self Service Portal installieren**.
3. Im Fenster **Aktuelle Versionen der Programme** wählen Sie aus und laden Sie die erforderliche Distribution über die Schaltfläche **Distribution herunterladen**.
4. Starten sie die heruntergeladene Datei.

   Der Assistent zum Entpacken der Distribution wird gestartet. Folgen Sie den Schritten des Assistenten.
5. Entpacken Sie die Distribution in den gewünschten Ordner.
6. Führen Sie im angegebenen Ordner die Datei install.exe aus.

   Der Assistent zur Installation von Anwendungen wird gestartet. Folgen Sie den Anweisungen.

Sie können auch die Datei setup.exe ausführen, die sich auf der CD-ROM des Programms Kaspersky Security Center 10 Web Console befindet.

Der Installationsvorgang des Self Service Portals von dem aus dem Internet heruntergeladenen Programmpaket stimmt mit dem Installationsvorgang von CD-ROM überein.

Schritt 1. Lizenzvertrag anzeigen

Machen Sie sich in diesem Schritt des Installationsassistenten mit dem Lizenzvertrag vertraut, den Sie mit Kaspersky Lab abschließen.

Lesen Sie den Endbenutzer-Lizenzvertrag sorgfältig durch. Wenn Sie mit allen Punkten der Vereinbarung einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**. Die Installation des Programms auf Ihrem Gerät wird fortgesetzt.

Falls Sie den Bedingungen des Lizenzvertrags nicht zustimmen, brechen Sie die Installation des Programms durch Klicken auf die Schaltfläche **Abbrechen** ab.

Die Remote-Installation des Self Service Portals mithilfe eines Installationspakets oder die lokale Installation im Silent-Modus setzt das automatische Einverständnis mit den Bedingungen des Lizenzvertrags für das zu installierende Programm voraus. Der Endbenutzer-Lizenzvertrag gehört zum Lieferumfang des Programms und kann in der Datei license.txt oder auf der Seite des technischen Supports von Kaspersky Lab angezeigt werden.

Schritt 2. Verbindung zu Kaspersky Security Center aufbauen

Wählen Sie die Verbindungsmethode zwischen Kaspersky Security Center und dem Self Service Portal. Es sind folgende Methoden verfügbar:

- **Auf einem lokalen Gerät installierten Apache-Server verwenden**: Bei Auswahl dieser Option erfolgt die Verbindung zwischen Self Service Portal und Kaspersky Security Center über einen Apache-Server, der auf dem Client-Gerät installiert wurde. (Die Installation eines Apache-Servers können Sie im nächsten Schritt des Assistenten auswählen.)

- **Auf einem Remote-Gerät installierten Apache-Server verwenden**: Sie können diese Variante auswählen, wenn ein Apache-Server auf dem Remote-Gerät mit der Linux-Plattform bereits installiert wurde. In diesem Fall wird nur der Serverteil von Self Service Portal lokal installiert. Um das Self Service Portal mit Kaspersky Security Center zu verbinden, muss auf dem Remote-Gerät der Client-Teil des Self Service Portals installiert werden. Bei Auswahl dieser Option wechselt der Installationsassistent zum 7. Schritt (s. Abschnitt "6. Schritt. Ports auswählen" auf S. 178).

► *Um den Client-Teil der Self Service Portal auf einem Remote-Gerät unter Linux zu installieren,*

starten Sie je nach Typ des Betriebssystems auf dem Remote-Gerät folgende Dateien:

- Für 32-Bit-Systeme:
  - kscwebconsole-10.<Versionsnummer>.i386.rpm
  - kscwebconsole_10.<Versionsnummer>_i386.deb.
- Für 64-Bit-Systeme:
  - kscwebconsole-10.<Versionsnummer>.x86_64.rpm
  - kscwebconsole_10.<Versionsnummer>_x86_64.deb.

Starten Sie die Datei mit der Erweiterung rpm, wenn auf dem Gerät ein rpm-basiertes Betriebssystem installiert ist. Starten Sie die Datei mit der Erweiterung deb, wenn auf dem Gerät ein deb-basiertes Betriebssystem installiert ist.

Schritt 3. Zielordner auswählen

Geben Sie den Installationsordner für das Self Service Portal an. Standardmäßig ist es der Ordner <Datenträger>:\Programme\Kaspersky Lab\Kaspersky Security Center Self Service Portal. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch erstellt. Sie können den Installationsordner mit der Schaltfläche **Durchsuchen** ändern.

Schritt 4. Installationsart für den Apache-Server auswählen

Wenn auf dem Gerät kein Apache-Server installiert ist, wird Ihnen in diesem Schritt des Installationsassistenten vorgeschlagen, den Apache HTTP-Server 2.4.25 zu installieren.

Standardmäßig ist die Installationsart Apache HTTP Server 2.4.25 aktiviert. Wenn Sie den Apache-Server nicht mithilfe des Installationsassistenten von Kaspersky Security Center 10 Web Console installieren wollen, deaktivieren Sie das Kontrollkästchen **Apache HTTP Server 2.4.25 installieren**.

> Während der Installation des Apache-Servers kann ein Neustart des Geräts erforderlich sein.

Schritt 5. Apache-Server installieren

In diesem Schritt des Assistenten wird der Apache HTTPS Server 2.4.25 installiert und konfiguriert.

Geben Sie vor der Installation das Zertifikat an, das das Self Service Portal für die Verbindung mit dem Apache-Server verwenden soll. Wählen Sie eine der folgenden Varianten aus:

- **Neues Zertifikat erstellen**. Neues Zertifikat für die Arbeit über das HTTPS-Protokoll erstellen. In diesem Fall wird für die Arbeit über das HTTPS-Protokoll ein selbstsigniertes Zertifikat erstellt.
- **Vorhandenes auswählen**. Ein vorhandenes Zertifikat für die Arbeit über das HTTPS-Protokoll verwenden. Legen Sie das Zertifikat auf eine der folgenden Weisen fest:
  - **Zertifikatsdatei auswählen**. Wählen Sie mithilfe der Schaltfläche **Durchsuchen** eine bestehende Zertifikatsdatei.
  - **Private Schlüsseldatei auswählen**: Geben Sie die private Schlüsseldatei der Zertifikats mithilfe der Schaltfläche **Durchsuchen** an.

Falls ein selbstsigniertes oder benutzerdefiniertes, nicht vertrauenswürdiges Zertifikat verwendet wird, kann auf einigen Geräten möglicherweise ein Zugangsproblem zum Self Service Portal auftreten. Das Problem kann durch die Installation des Stammzertifikats in der Liste der auf dem Gerät vertrauenswürdigen Zertifikate gelöst werden.

Sie können das Self Service Portal erforderlichenfalls so konfigurieren, dass es nicht über das HTTPS-Protokoll sondern über das HTTP-Protokoll ausgeführt wird. Detaillierte Informationen über die Ausführung des Self Service Portals über das HTTP-Protokoll finden Sie in der Wissensdatenbank des Technischen Supports von Kaspersky Lab unter http://support.kaspersky.com/de/11452.

Nachdem Sie das Zertifikat ausgewählt haben, klicken Sie auf **Weiter**. Daraufhin wird die Installation des Apache HTTPS-Servers 2.4.25 gestartet. Folgen Sie den Anweisungen des Assistenten.

Schritt 6. Ports auswählen

Passen Sie die folgenden Einstellungen an:

- SSL-Portnummer für die geschützte Verbindung des Geräts mit dem Administrationsserver. Standardmäßig wird Port 13291 verwendet.
- Portnummer für die Verbindung des Geräts mit dem Apache-Server. Standardmäßig wird Port 9000 verwendet.
- Adresse des Geräts, auf dem der Administrationsserver installiert ist.
  In der Standardeinstellung ist die Adresse localhost festgelegt.

  Wenn sich das Gerät, auf das Kaspersky Security Center 10 Web Console installiert wird und Self Service Portal, in einer entmilitarisierten Zone befindet, aktivieren Sie das Kontrollkästchen **Verbindungs-Gateway** und geben Sie im Feld **Serveradresse** die Adresse des Verbindungs-Gateways an.
- Portnummer für die Verbindung des Geräts mit der Kaspersky Security Center 10 Web Console. Standardmäßig wird Port 8080 verwendet.
- Portnummer für die Verbindung des Geräts mit dem Self Service Portal.
  Standardmäßig wird Port 8081 verwendet.

Nach der Installation von Kaspersky Security Center 10 Web Console und Self Service Portal können Sie die standardmäßig festgelegten Portnummern ändern (s. Abschnitt "Portnummer der Verbindung des Geräts ändern" auf S. 97).

Schritt 7. Benutzerkonto auswählen

Geben Sie das Domain-Benutzerkonto des Benutzers an, unter dem mithilfe von QR-Codes Installationspakete auf die mobilen Geräte der Benutzer heruntergeladen werden.
Das Benutzerkonto muss im Format <*Domain-Name*>\<*Kontoname*> angegeben werden.

Über die Schaltfläche **Test** können Sie die Verbindung mit dem Administrationsserver prüfen.

Schritt 8. Installation des Self Service Portals starten

Klicken Sie auf die Schaltfläche **Beginnen**, um die Installation des Self Service Portals zu starten.

Der Installationsvorgang wird im Fenster des Assistenten angezeigt.

Schritt 9. Installation des Self Service Portals beenden

Wenn vor der Installation des Self Service Portals auf dem Gerät bereits ein Apache Server Version 2.4.25 oder höher installiert wurde oder die automatische Installation des Apache-Servers fehlerhaft beendet wurde, wird Ihnen in diesem Schritt des Assistenten vorgeschlagen, die Datei mit den Anweisungen zur Konfiguration des Apache-Servers zu öffnen. Um die Textdatei mit den Anweisungen nach Abschluss des Assistenten anzuzeigen, aktivieren Sie das Kontrollkästchen **Die Datei readme.txt öffnen**.

Um den Installationsassistenten abzuschließen, klicken Sie auf **Fertig**.

SMS-Versand in Kaspersky Security Center konfigurieren

Kaspersky Security Center kann für den Versand von SMS-Nachrichten an Benutzer von mobilen Geräten verwendet werden.

Der SMS-Versand kann in folgenden Fällen verwendet werden:

- Damit der Administrator SMS-Nachrichten über Ereignisse in der Funktionsweise des Administrationsservers und der Programme erhält, die auf Client-Geräten installiert sind.
- Damit Programme auf den mobilen Geräten der Benutzer installiert werden Der Benutzer eines mobilen Gerätes erhält eine SMS mit dem Link zum Herunterladen eines Programms, das installiert werden soll.
- Damit Mitarbeiter des Unternehmens benachrichtigt werden.

Die Bereitstellung des SMS-Versands erfolgt in folgender Reihenfolge:

1. Der Administrator installiert das Tool Kaspersky SMS Broadcasting auf dem mobilen Android-Gerät.

   > Das Tool Kaspersky SMS Broadcasting wird ausschließlich auf mobilen Geräten auf der Android-Plattform installiert.

2. Nachdem das Tool Kaspersky SMS Broadcasting auf dem mobilen Gerät installiert wurde, synchronisiert der Administrator das mobile Gerät mit dem Administrationsserver.
3. Der Administrator legt in der Verwaltungskonsole ein mobiles Gerät, auf dem das Tool Kaspersky SMS Broadcasting installiert ist, als SMS-Versender fest.

In diesem Abschnitt

Tool Kaspersky SMS Broadcasting erhalten und installieren

Das Tool Kaspersky SMS Broadcasting ist Teil des Installationspakets von Kaspersky Security 10 für mobile Endgeräte. Sie können das Installationspaket von Kaspersky Security 10 für mobile Endgeräte von der Website von Kaspersky Lab laden.

► *Gehen Sie wie folgt vor, um das Tool Kaspersky SMS Broadcasting zu installieren:*

1. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** den Unterordner **Installationspakete** aus.

   Der Ordner **Remote-Installation** befindet sich standardmäßig im Ordner **Erweitert**.

2. Klicken Sie auf die Schaltfläche **Erweiterte Aktionen** und wählen Sie aus der daraufhin angezeigten Liste den Punkt **Pakete für mobile Apps verwalten**.

3. Wählen Sie im Fenster **Pakete für mobile Apps verwalten** das Paket für mobile Anwendungen aus, das das Tool Kaspersky SMS Broadcasting enthält.

   Wurde kein Paket erstellt, klicken Sie auf die Schaltfläche **Neu** und erstellen Sie ein Paket für mobile Anwendungen für das Tool Kaspersky SMS Broadcasting.

4. Klicken Sie im Fenster **Pakete für mobile Apps verwalten** auf die Schaltfläche **Auf dem Webserver veröffentlichen**.

   Der Link zum Herunterladen des Pakets für mobile Anwendungen mit dem Tool Kaspersky SMS Broadcasting wird auf dem Web-Server veröffentlicht.

5. Klicken Sie im Fenster **Pakete für mobile Apps verwalten** auf die Schaltfläche **Versenden**, um dem Benutzer eines mobilen Geräts einen Link zum Herunterladen des Pakets für mobile Anwendungen zu senden, das das Tool Kaspersky SMS Broadcasting enthält.

6. Laden Sie das Paket für mobile Anwendungen, das das Tool Kaspersky SMS Broadcasting enthält, vom Web-Server auf das mobile Gerät herunter.

7. Führen Sie die Installation des Tools Kaspersky SMS Broadcasting mithilfe der normalen Tools des mobilen Gerätes aus.

Sie können das Tool Kaspersky SMS Broadcasting auch auf das mobile Gerät von der Website von Kaspersky Lab herunterladen oder das mobile Gerät an ein Client-Gerät anschließen und das bereits heruntergeladene Tool Kaspersky SMS Broadcasting auf das mobile Gerät kopieren.

Mobiles Gerät mit dem Administrationsserver synchronisieren

► *Um das mobile Gerät mit dem Administrationsserver zu synchronisieren, gehen Sie folgendermaßen vor:*

1. Klicken Sie in der Konsolenstruktur von Kaspersky Security Center mit der rechten Maustaste auf den Ordner **Administrationsserver** und wählen Sie den Punkt **Eigenschaften** aus.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktiveren Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Einstellungen** das Kontrollkästchen **Port für mobile Geräte öffnen**.

3. Geben Sie im Abschnitt **Einstellungen** im Feld **Port für mobile Geräte** den Port für die Synchronisierung des mobilen Gerätes mit dem Administrationsserver an. Standardmäßig wird Port 13292 verwendet.

4. Starten Sie das Tool Kaspersky SMS Broadcasting auf dem mobilen Gerät.

5. Klicken Sie im Hauptfenster des Tools Kaspersky SMS Broadcasting auf die Schaltfläche **Synchronisierungs-Einstellungen**.

6. Geben Sie im Fenster **Synchronisierungs-Einstellungen** im Feld **Serveradresse** die IP-Adresse des Administrationsservers an.

7. Geben Sie im Feld **Port** den Port für die Verbindung zum Administrationsserver an. Standardmäßig wird Port 13292 verwendet.

8. Klicken Sie auf die Schaltfläche **OK**.

Wenn das mobile Gerät mit dem Administrationsserver synchronisiert wird, können Sie dieses mobile Gerät als Versender von SMS-Nachrichten festlegen.

Mobiles Gerät als Versender von SMS-Nachrichten festlegen

► *Um das mobile Gerät als Versender von SMS-Nachrichten festzulegen, gehen Sie folgendermaßen vor:*

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Wählen Sie im Arbeitsplatz des Knotens die Registerkarte **Ereignisse** aus.

3. Wählen Sie mithilfe des Links **Benachrichtigungseinstellungen und Ereignis-Export anpassen** in der Dropdown-Liste die Option **SMS-Absenderliste anpassen**.

   Das Eigenschaftenfenster für Ereignisse wird im Abschnitt **SMS-Absender** geöffnet.

4. Klicken Sie im Abschnitt **SMS-Absender** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Gerät auswählen** wird geöffnet.

5. Geben Sie im Fenster **Gerät auswählen** das mobile Gerät an, das als Versender von SMS-Nachrichten verwendet wird.

6. Klicken Sie auf die Schaltfläche **OK**.

Auf dem Gerät, das als Absender von SMS-Nachrichten festgelegt ist, muss das Tool Kaspersky SMS Broadcasting installiert sein.

Netzwerkbelastung

Diesem Abschnitt können Informationen über den Umfang des Datenverkehrs im Netzwerk entnommen werden, mit dem zwischen den Client-Geräten und dem Administrationsserver bei wichtigen administrativen Vorgängen Daten ausgetauscht werden.

Die Grundbelastung des Netzwerks hängt mit folgenden Szenarios zusammen:

- Erstmalige Softwareverteilung des Antiviren-Schutzes
- Erstmaliges Update der Antiviren-Datenbanken
- Synchronisierung des Client-Geräts mit dem Administrationsserver
- Regelmäßiges Update der Antiviren-Datenbanken
- Verarbeitung von Ereignissen auf Client-Geräten durch Administrationsserver.

In diesem Abschnitt

Erstmalige Softwareverteilung des Antiviren-Schutzes

Diesem Abschnitt können Informationen zum verbrauchten Datenvolumen bei der Installation des Administrationsagenten 10 und Kaspersky Endpoint Security 10 für Windows auf dem Client-Gerät entnommen werden (s. Tabelle unten).

Der Administrationsagent wird mit der erzwungenen Installation installiert, wenn der Administrationsserver die für die Installation benötigten Dateien in den gemeinsamen Ordner auf dem Client-Gerät kopiert hat. Nach der Installation empfängt der Administrationsagent über die Verbindung mit dem Administrationsserver das Programmpaket von Kaspersky Endpoint Security 10 für Windows.

Tabelle 10. Datenverkehr

Szenario	Installation des Administrations-agenten für ein Client-Gerät	Installation von Kaspersky Endpoint Security 10 für Windows für ein Client-Gerät (mit den aktualisierten Datenbanken)	Gemeinsame Installation des Administrations-agenten und Kaspersky Endpoint Security 10 für Windows
Datenverkehr vom Client-Gerät zum Administrations-server, KB	386,70	1.841,3	2.253,8
Datenverkehr vom Administrations-server zum Client-Gerät, KB	14.801,13	269.994,5	284.768,7
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	15.187,83	271.835,8	287.022,5

Nach der Installation der Administrationsagenten lässt sich auf den gewünschten Client-Geräten ein Gerät in der Administrationsgruppe als Update-Agent einrichten. Er wird für das Verteilen der Installationspakete verwendet. In diesem Fall kann sich die bei erstmaliger Softwareverteilung des Antiviren-Schutzes zu übertragende Datenmenge in Abhängigkeit davon, ob die Option IP-Multicast eingesetzt wird, ganz erheblich unterscheiden.

Bei dieser Option werden die Installationspakete einmal an alle in der Administrationsgruppe eingeschalteten Geräte verschickt. So wird der gesamte Datenverkehr ungefähr um das N-fache verringert, wobei N der Anzahl der eingeschalteten Geräte in der Administrationsgruppe entspricht. Wenn IP-Multicast nicht verwendet wird, stimmt der gesamte Datenverkehr mit dem Datenverkehr beim Download der Installationspakete vom Administrationsserver überein. Als Quelle für den Download der Installationspakete dient nicht der Administrationsserver, sondern der Update-Agent.

Erstmaliges Update der Antiviren-Datenbanken

Diesem Abschnitt können Informationen zum verbrauchten Datenvolumen beim ersten Start Aufgabe zum Datenbanken-Update auf dem Client-Gerät entnommen werden (s. Tabelle unten). Die in der Tabelle aufgeführten Daten können je nach Datenbankversion etwas abweichen.

Tabelle 11. Datenverkehr

Szenario	Erstmaliges Update der Antiviren-Datenbanken
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	1.357,1
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	33.917,0
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	35.274,1

Synchronisierung des Clients mit dem Administrationsserver

Dieses Szenario charakterisiert den Zustand des Administrationssystems, in dem die Daten zwischen dem Client-Gerät und dem Administrationsserver aktiv synchronisiert werden. Die Client-Geräte stellen innerhalb der durch den Administrator vorgegebenen Fristen eine Verbindung zum Administrationsserver her. Der Administrationsserver vergleicht den Datenzustand auf dem Client-Gerät mit dem Datenzustand auf dem Server, registriert die Daten über die letzte Verbindung des Client-Geräts in der Datenbank und synchronisiert die Daten.

Diesem Abschnitt können Informationen zum Datenverkehr in die wichtigsten administrativen Szenarios bei der Verbindung des Clients mit dem Administrationsserver mit Synchronisierung entnommen werden (s. Tabelle unten). Die in der Tabelle aufgeführten Daten können je nach Datenbankversion etwas abweichen.

Tabelle 12. Datenverkehr

Szenario	Datenverkehr von Client-Geräten zum Administrationsserver, KB	Datenverkehr vom Administrationsserver zu den Client-Geräten, KB	Allgemeiner Datenverkehr (für ein Client-Gerät), KB
Erstmalige Synchronisierung vor dem Datenbanken-Update auf dem Client-Gerät	368,6	463,7	832,3
Erstmalige Synchronisierung nach dem Datenbanken-Update auf dem Client-Gerät	1.748,3	34.388,3	36.136,6
Synchronisierung bei fehlenden Änderungen auf dem Client-Gerät und auf dem Administrationsserver	8,7	6,6	15,3
Synchronisierung bei Änderung einer Einstellung in der Gruppenrichtlinie	11,1	13,3	24,4
Synchronisierung bei Änderung einer Einstellung in der Gruppenaufgabe	10,0	12,5	22,5
Erzwungene Synchronisierung bei fehlenden Änderungen auf dem Client-Gerät	47,3	15,5	62,8

Der Umfang des allgemeinen Datenverkehrs unterscheidet sich in Abhängigkeit davon, ob die Option IP-Multicast innerhalb der Administrationsgruppen eingesetzt wird, ganz erheblich. Bei Einsatz von IP-Multicast verringert sich der gesamte Datenverkehr in eine Gruppe ungefähr um das N-fache, wobei N der Anzahl der aktivierten Geräte in der Administrationsgruppe entspricht.

Der Umfang des Verkehrs bei der erstmaligen Synchronisierung vor und nach dem Datenbanken-Update wird für folgende Fälle angegeben:

- Installation des Administrationsagenten und des Schutzprogramms auf dem Client-Gerät
- Verschieben des Client-Geräts in die Administrationsgruppe
- Anwendung der standardmäßig für die Gruppe erstellten Richtlinien und Aufgaben auf das Client-Gerät.

In der Tabelle wird der Umfang des Datenverkehrs bei der Veränderung einer der Schutzeinstellungen angezeigt, die zu den Richtlinieneinstellungen von Kaspersky Endpoint Security gehören. Die Daten für andere Richtlinieneinstellungen können sich von den in der Tabelle dargestellten Daten unterscheiden.

Zusätzliches Update der Antiviren-Datenbanken

Diesem Abschnitt können Informationen zum Datenverkehr bei einem inkrementellen Update der Antiviren-Datenbanken entnommen werden, das 20 Stunden nach dem letzten Update erfolgt (s. Tabelle unten). Die in der Tabelle aufgeführten Daten können je nach Datenbankversion etwas abweichen.

Tabelle 13. Datenverkehr

Szenario	Inkrementelles Update der Antiviren-Datenbanken
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	436,9
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	9.979,2
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	10.416,1

Der Umfang des Datenverkehrs unterscheidet sich in Abhängigkeit davon, ob die Option IP-Multicast innerhalb der Administrationsgruppen eingesetzt wird, ganz erheblich. Bei Einsatz von IP-Multicast verringert sich der gesamte Datenverkehr in eine Gruppe ungefähr um das N-fache, wobei N der Anzahl der aktivierten Geräte in der Administrationsgruppe entspricht.

Verarbeitung von Ereignissen der Clients durch Administrationsserver

Diesem Abschnitt können Informationen zum Datenverkehr auf einem Client-Gerät bei Eintritt des Ereignisses "Virus gefunden" entnommen werden, dessen Daten an den Administrationsserver übertragen und in der Datenbank registriert werden (siehe Tabelle unten).

Tabelle 14. Datenverkehr

Szenario	Übertragen von Daten an Administrationsserver bei Eintreten des Ereignisses "Virus gefunden"	Übertragen von Daten an Administrationsserver bei Eintreten von neun Ereignissen "Virus gefunden"
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	27,2	100,4
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	25,8	52,5
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	53,0	152,9

Die in der Tabelle aufgeführten Daten können in Abhängigkeit von der verwendeten Version des Antiviren-Programms und davon, welche Ereignisse in der Richtlinie in der Datenbank des Administrationsservers als erfassungswürdig definiert sind, etwas abweichen.

Datenverkehr in 24 Stunden

Diesem Abschnitt können Informationen zum verbrauchten Datenvolumen für 24 Stunden entnommen werden, in den sich das Administrationssystem im Ruhezustand befindet, wenn keine Änderungen von der Seite der Client-Geräte oder des Administrationsservers vorgenommen wurden (s. Tabelle unten).

Die in der Tabelle aufgeführten Daten erläutern den Netzwerkstatus nach der Standardinstallation von Kaspersky Security Center und Fertigstellung des Schnellstartassistenten.
Das Synchronisierungsintervall des Client-Geräts mit dem Administrationsserver betrug 20 Minuten, der Update-Download in die Datenverwaltung des Administrationsservers erfolgte stündlich.

Tabelle 15. Datenverkehr

Szenario	Ruhezustand des Administrationssystems
Datenverkehr vom Client-Gerät zum Administrationsserver, KB	2.162,2
Datenverkehr vom Administrationsserver zum Client-Gerät, KB	51.000,2
Allgemeiner Datenverkehr (für ein Client-Gerät), KB	53.162,4

Geschwindigkeit, mit der die Datenbank mit den Ereignissen von Kaspersky Endpoint Security gefüllt wird

In diesem Abschnitt werden Beispiele für die Geschwindigkeit aufgeführt, mit der die Datenbank des Administrationsservers mit Ereignissen gefüllt wird, die sich beim Ausführen von verwalteten Programmen ergeben.

Informationen über Ereignisse in der Funktionsweise der verwalteten Programme werden vom Client-Gerät übertragen und in der Datenbank des Administrationsservers registriert.

In der Datenbank werden (Ne*Nh) Ereignisse pro Tag registriert (s. Tabelle unten), wobei Nh der Anzahl von Client-Geräten, auf denen verwaltete Programme installiert wurden, und Ne der Anzahl von Ereignissen pro Tag entspricht, deren Informationen das auf dem Client-Gerät installierte verwaltete Programm überträgt.

Tabelle 16. Geschwindigkeit, mit der die Datenbank mit den Ereignissen gefüllt wird

Anzahl von Geräten, auf denen verwaltete Programme installiert sind	Anzahl von Ereignissen pro Tag, die in die Datenbank eingetragen werden
100	≤ 2000
1000	≤ 20.000
10.000	≤ 200.000

In der Tabelle sind Daten für den normalen Modus von verwalteten Programmen aufgeführt, bei dem für ein Client-Gerät maximal 20 Ereignisse pro Tag registriert werden.

Die maximale Anzahl von Ereignissen, die in der Datenbank gespeichert werden, wird im Abschnitt **Ereignisse speichern** des Eigenschaftenfensters des Administrationsservers festgelegt. Standardmäßig werden in der Datenbank maximal 400.000 Ereignisse gespeichert.

Anfrage an den Technischen Support

Dieser Abschnitt beschreibt, wie Sie technischen Support erhalten können, und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

In diesem Abschnitt

Kontakt zum Technischen Support

Wenn Sie in der Programmdokumentation und in den anderen Informationsquellen zum Programm (s. Abschnitt "Informationsquellen zum Programm" auf S. 14) keine Lösung für Ihr Problem finden können, empfiehlt es sich, sich an den Technischen Support zu wenden. Die Mitarbeiter 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 Nutzung des Programms erworben haben. Benutzer mit einer Testlizenz erhalten keinen technischen Support.

Bitte lesen Sie die Regeln für die Nutzung des Technischen Supports (http://support.kaspersky.com/de/support/rules), bevor Sie sich an diesen wenden.

Eine Kontaktaufnahme mit den Experten des Technischen Supports ist auf folgende Weise möglich:

- Anruf beim Technischen Support (http://support.kaspersky.com/de/b2b)
- Versand einer Anfrage an den Technischen Support von Kaspersky Lab über das Portal Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Telefonischer technischer Support

In den meisten Regionen der Welt können Sie den Technischen Support telefonisch erreichen. Informationen über die Möglichkeiten des Technischen Supports in Ihrer Region sowie dessen Kontaktadressen finden Sie auf der Website des Technischen Supports von Kaspersky Lab (http://support.kaspersky.com/de/b2b).

> Bitte beachten Sie die Support-Richtlinien (http://support.kaspersky.com/de/support/rules), bevor Sie sich an den Technischen Support wenden.

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount(https://companyaccount.kaspersky.com) ist ein Portal für Unternehmen, die Kaspersky-Lab-Programme verwenden. Das Portal Kaspersky CompanyAccount dient der Interaktion zwischen Benutzern und Kaspersky-Lab-Experten mithilfe von E-Mail-Anfragen. Auf dem Portal Kaspersky CompanyAccount können Sie den Status der Bearbeitung von E-Mail-Anfragen durch die Kaspersky-Lab-Experten verfolgen und den Verlauf der E-Mail-Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Benutzerkontos können Sie die Online-Anfragen der bei Kaspersky Lab registrierten Mitarbeiter zentral verwalten und die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

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

Weitere Informationen über Kaspersky CompanyAccount finden Sie auf der Website des Technischen Supports (http://support.kaspersky.com/de/faq/companyaccount_help).

Glossar

A

Administrationsagent

Der Administrationsagent ist eine Komponente des Programms Kaspersky Security Center und für die Kommunikation zwischen dem Administrationsserver und den Kaspersky-Lab-Anwendungen zuständig, die auf einem konkreten Netzwerkknoten (Workstation oder Server) installiert sind. Diese Komponente ist für alle unter Windows laufenden Programme des Unternehmens einheitlich. Für Kaspersky-Lab-Anwendungen für Novell, Unix und Mac gibt es spezielle Versionen des Administrationsagenten.

Administrationsgruppe

Eine Reihe von Geräten, die entsprechend der auszuführenden Funktionen und der auf ihnen installierten Programme von Kaspersky Lab zusammengefasst wurden. Die Gruppierung erfolgt zur einfachen Verwaltung der Geräte als geschlossene Einheit. Zu einer Gruppe können andere Gruppen gehören. Für alle in der Gruppe installierten Anwendungen können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

Administrationsserver

Komponente von Kaspersky Security Center, welche die Funktionen zum zentralen Speichern von Daten über die im Unternehmensnetzwerk installierten Kaspersky-Lab-Anwendungen und deren Verwaltung ausführt.

Administrator-Arbeitsplatz

Gerät, auf dem eine Komponente installiert ist, die eine Schnittstelle für die Programmverwaltung bereitstellt. Für Antiviren-Produkte ist das die Konsole des Anti-Virus, für das Programm Kaspersky Security Center – die Verwaltungskonsole.

Vom Administrator-Arbeitsplatz aus wird der Serverteil des Programms konfiguriert und verwaltet. Für Kaspersky Security Center erfolgt der Aufbau und die Verwaltung eines zentralen Antiviren-Schutz-Systems für das Unternehmensnetzwerk, dem Kaspersky-Lab-Anwendungen zugrunde liegen.

Aktiver Schlüssel

Schlüssel, der im Augenblick für die Programmausführung verwendet wird.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die den Kaspersky-Lab-Experten zum Zeitpunkt der Erscheinung der Antiviren-Datenbanken bekannt sind. Die Einträge in den Antiviren-Datenbanken ermöglichen das Erkennen von schädlichem Code in den zu untersuchenden Objekten. Die Antiviren-Datenbanken werden von den Kaspersky-Lab-Experten erstellt und stündlich aktualisiert.

Anwendungseinstellungen

Einstellungen des Programms, die für alle Aufgabenarten gleich sind und sich auf die Funktion des Programms insgesamt beziehen, zum Beispiel die Einstellungen der Leistungsfähigkeit der Anwendung, die Einstellungen für die Berichtsführung und die Backup-Einstellungen.

Aufgabe

Funktionen, die ein Kaspersky-Lab-Programm in Form von Aufgaben ausführt, zum Beispiel: Echtzeitschutz für Dateien, Vollständige Untersuchung des Geräts, Datenbanken-Update.

Aufgabe für bestimmte Geräte

Aufgabe, die für mehrere Client-Geräte aus beliebigen Administrationsgruppen festgelegt wurde und auf diesen auszuführen ist.

Aufgabeneinstellungen

Einstellungen des Programms, die für jede Aufgabenart spezifisch sind.

B

Backup für Sicherungskopien

Spezieller Ordner für die Speicherung von Kopien der Daten des Administrationsservers, die mit dem Sicherungs- u. Wiederherstellungstool angelegt worden sind.

C

Client des Administrationsservers (Client-Gerät)

Gerät (Server oder Arbeitsstation), auf dem der Administrationsagent und die zu verwaltenden Kaspersky-Lab-Programme installiert sind.

E

EAS-Gerät

Ein mobiles Gerät, das mit dem Administrationsserver mit dem Exchange ActiveSync-Protokoll verbunden wird.

Ereigniskategorie des Ereignisses

Eigenschaften eines Ereignisses, das in der Kaspersky-Lab-Anwendung erfasst worden ist. Vier Ereigniskategorien sind verfügbar:

- Kritisches Ereignis.
- Funktionsfehler.

- Warnung.
- Infomeldung.

Ereignisse des gleichen Typs können verschiedene Ereigniskategorien aufweisen, da sie von der Situation abhängig ist, in der das Ereignis eingetreten ist.

Erzwungene Installation

Mit dieser Methode der Remote-Installation von Kaspersky Lab-Anwendungen kann ein Programm auf konkrete Client-Geräte installiert werden. Um eine Aufgabe mit der erzwungenen Installation erfolgreich auszuführen, muss das Benutzerkonto für den Start der Aufgabe über Berechtigungen für den Remote-Start von Programmen auf den Client-Geräten verfügen. Diese Methode eignet sich für die Installation von Anwendungen auf Geräten, die unter den Betriebssystemen Microsoft Windows NT/2000/2003/XP laufen, bei welchen diese Option unterstützt wird, oder auf Geräten mit den Betriebssystemen Microsoft Windows 98/Me, auf welchen der Administrationsagent installiert ist.

Exchange ActiveSync-Server für mobile Geräte

Eine Komponente von Kaspersky Security Center, die eine Verbindung von Exchange ActiveSync-Mobilgeräten mit dem Administrationsserver ermöglicht.
Wird auf dem Client-Gerät installiert.

G

Gruppenaufgabe

Aufgabe für eine Administrationsgruppe. Wird auf allen Client-Geräten ausgeführt, die zu dieser Administrationsgruppe gehören.

Gültigkeitsdauer der Lizenz

Zeitraum, in dem Sie Programmfunktionen und zusätzliche Leistungen nutzen können. Der verfügbare Funktionsumfang sowie der Umfang der zusätzlichen Leistungen werden durch den Lizenztyp definiert.

I

Inkompatibles Programm

Ein Antiviren-Programm eines Drittherstellers oder ein Kaspersky-Lab-Programm, das die Verwaltung über Kaspersky Security Center nicht unterstützt.

Installation mit Anmeldeskript

Mit dieser Methode der Remote-Installation von Kaspersky-Lab-Anwendungen kann der Start der Aufgabe Remote-Installation mit einem konkreten Benutzerkonto (mehrerer Benutzer) verknüpft werden. Bei der Anmeldung des Benutzers in der Domäne wird versucht, die Anwendung auf dem Client-Gerät zu installieren, von dem aus sich der Benutzer registriert hat. Diese Methode eignet sich für die Installation von Anwendungen auf Geräten, die unter dem Betriebssystem Microsoft Windows 98/Me laufen.

Installationspaket

Eine Gruppe von Dateien, die zur Remote-Installation von Kaspersky-Lab-Anwendungen mit der Remote-Administration von Kaspersky Security Center angelegt wird. Das Installationspaket enthält eine Auswahl von Einstellungen, die für die Programminstallation und die Gewährleistung seiner problemlosen Ausführung sofort nach der Installation erforderlich sind. Die Einstellungen entsprechen der Standardkonfiguration der Anwendung. Das Installationspaket wird auf der Grundlage von Dateien mit den Erweiterungen kpd und kud erstellt, die zur Programmdistribution gehören.

iOS MDM-Gerät

Ein mobiles iOS-Gerät, das durch den iOS MDM-Server verwaltet wird (s. Abschnitt "iOS MDM-Server" auf S. 202).

iOS MDM-Server

Eine Komponente von Kaspersky Security Center, die auf einem Client-Gerät installiert wird. Sie ermöglicht die Verbindung von mobilen iOS-Geräten mit dem Administrationsserver und ihre Verwaltung mithilfe des Dienstes Apple Push Notifications (APNs).

iOS MDM-Profil

Auswahl von Einstellungen für die Verbindung von Mobilgeräten mit dem Administrationsserver. Das iOS MDM-Profil wird vom Benutzer auf das mobile Gerät installiert. Anschließend stellt das Mobilgerät eine Verbindung zum Administrationsserver her.

K

Kaspersky-Lab-Updateserver

HTTP-Server von Kaspersky Lab, von denen die Programme Datenbanken-Updates und Updates von Programm-Modulen erhalten.

Kaspersky Security Center Administrator

Dabei handelt es sich um eine Person, welche die Anwendung über Kaspersky Security Center, das zentrale System zur Remote-Administration, steuert.

Kaspersky Security Center System Health Validator (SHV)

Eine Komponente des Programms Kaspersky Security Center, die für die Prüfung der Funktionstüchtigkeit des Betriebssystems beim gleichzeitigen Einsatz des Programms Kaspersky Security Center mit Microsoft NAP vorgesehen ist.

Kaspersky Security Center Webserver

Eine Komponente von Kaspersky Security Center, die zusammen mit dem Administrationsserver installiert wird. Der Webserver dient dazu, autonome Installationspakete, iOS MDM-Profile sowie Dateien aus einem freigegebenen Ordner im Netzwerk zu übertragen.

Konfigurationsprofil

Richtlinie, die Einstellungen und Einschränkungen für ein mobiles iOS MDM-Gerät umfasst.

L

Lokale Aufgabe

Aufgabe, die für ein einzelnes Client-Gerät festgelegt wurde und darauf ausgeführt werden soll.

O

Operator von Kaspersky Security Center SPE

Ein Benutzer, der die Kontrolle über den Status und die Funktion des Antiviren-Schutzsystems übernimmt, das mithilfe von Kaspersky Security Center verwaltet wird.

P

Profil

Eine Gruppe von Einstellungen, die das Verhalten der Exchange ActiveSync-Mobilgeräte bei der Verbindung mit dem Microsoft Exchange-Server definieren.

Provisioning-Profil

Eine Gruppe von Einstellungen für die Funktion der Apps auf mobilen iOS-Geräten. Ein Provisioning-Profil enthält Informationen zur Lizenz und ist mit einer bestimmten App verbunden.

R

Remote-Installation

Installation von Kaspersky Lab-Anwendungen mit Diensten, die Kaspersky Security Center zur Verfügung stellt.

Reserveschlüssel

Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen für die Ausführung des Programms sowie den Zugriff auf die Programmeinstellungen, die auf den Geräten der Administrationsgruppe installiert sind. Für jedes Programm muss eine eigene Richtlinie erstellt werden. Sie können eine unbegrenzte Anzahl von verschiedenen Richtlinien für die Programme erstellen, die auf den Geräten jeder Administrationsgruppe installiert sind. Im Rahmen einer Administrationsgruppe kann jedoch für jedes Programm immer nur eine Richtlinie gleichzeitig angewendet werden.

S

Schlüsseldatei

Datei mit der Form xxxxxxxx.key, die es ermöglicht, Kaspersky-Lab-Programme mit einer Testlizenz oder mit einer kommerziellen Lizenz zu nutzen. Sie können das Programm nur verwenden, wenn Sie über eine Schlüsseldatei verfügen.

Schutzstatus

Der Schutzstatus gibt den aktuellen Zustand des Schutzes an, der das Sicherheitsniveau des Geräts charakterisiert.

Schwellenwert für Virenaktivität

Maximal zulässige Anzahl an Ereignissen einer bestimmten Art in festgelegter Zeit, bei deren Überschreiten von einer vermehrten Virenaktivität ausgegangen und die Bedrohung Virenangriff ausgelöst wird. Diese Funktion hat bei Virenepidemien eine große Bedeutung und ermöglicht Administratoren, rechtzeitig auf Bedrohungen durch Virenangriffe zu reagieren.

Server für mobile Geräte

Eine Komponente von Kaspersky Security Center, die den Zugriff auf mobile Geräte bereitstellt und deren Verwaltung über die Verwaltungskonsole ermöglicht.

Sicherungskopie der Daten des Administrationsservers erstellen

Die Daten des Administrationsservers werden als Backup und zur Wiederherstellung mit dem Sicherungs- u. Wiederherstellungstool gespeichert. Das Tool kann Folgendes speichern:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse);
- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte;

- Datenverwaltung der Programmdistributionen für die Remote-Installation (Inhalt der Ordner Packages, Uninstall, Updates);
- Zertifikat des Administrationsservers.

U

Unmittelbare Programmverwaltung

Programmverwaltung über eine lokale Schnittstelle.

Update

Vorgang zum Ersetzen bestehender bzw. Hinzufügen neuer Dateien (Datenbanken oder Programm-Module), die von den Kaspersky-Lab-Update-Servern heruntergeladen wurden.

Update-Agent

Gerät mit installiertem Administrationsagenten, der für das Verteilen von Updates, die Remote-Installation von Programmen, das Empfangen von Informationen über Geräte, die Teil einer Administrationsgruppe und/oder einer Broadcast-Domäne sind, verwendet wird. Update-Agenten dienen zur Verringerung der Belastung auf dem Administrationsserver bei der Verteilung von Updates und zur Optimierung des Netzwerkverkehrs. Update-Agenten können automatisch durch den Administrationsserver oder manuell durch den Administrator bestimmt werden.

V

Verfügbares Update

Paket von Updates für die Module der Kaspersky-Lab-Anwendung, zu welchem dringende Updates, die während eines bestimmten Zeitraums gesammelt wurden, und Änderungen an der Programmarchitektur gehören.

Verwaltungskonsole

Eine Komponente von Kaspersky Security Center, die eine Benutzeroberfläche für die Administrationsdienste des Administrationsservers und des Administrationsagenten bietet.

Verwaltungs-Plug-in für das Programm

Spezielle Komponente, die die Schnittstelle für die Programmsteuerung durch die Verwaltungskonsole bereitstellt. Jedes Programm verfügt über sein eigenes Verwaltungs-Plug-in. Die Komponente gehört zu allen Kaspersky-Lab-Anwendungen, deren Verwaltung mit Kaspersky Security Center möglich ist.

W

Wiederherstellen der Daten des Administrationsservers

Das Wiederherstellen der Daten des Administrationsservers erfolgt mithilfe des Sicherungs- u. Wiederherstellungstools auf Grundlage der Daten, die im Backup gespeichert sind. Mit dem Tool kann Folgendes wiederhergestellt werden:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse);
- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte;

- Datenverwaltung der Programmdistributionen für die Remote-Installation (Inhalt der Ordner Packages, Uninstall, Updates);
- Zertifikat des Administrationsservers.

Z

Zentrale Programmverwaltung

Remote-Programmverwaltung mit den Administrationsdiensten, die Kaspersky Security Center zur Verfügung stellt.

Zertifikat des Administrationsservers

Mit diesem Zertifikat wird der Administrationsserver bei seinem Verbindungsaufbau zur Verwaltungskonsole und beim Datenaustausch mit den Client-Geräten authentifiziert. Das Zertifikat des Administrationsservers wird bei der Installation des Administrationsservers angelegt und auf dem Administrationsserver im Unterordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert gespeichert.

AO Kaspersky Lab

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen zum Schutz von Computern vor den verschiedensten Arten von Bedrohungen, insbesondere Schutz vor Viren und anderer Schadsoftware, unerwünschten Nachrichten (Spam), Netzwerk- und Hackerangriffen.

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"). In Russland ist Kaspersky Lab laut IDC der bevorzugte Hersteller von Systemen zum Schutz von Computern für Heimanwender ("IDC Endpoint Tracker 2014").

Kaspersky Lab wurde 1997 in Russland gegründet. Heute ist Kaspersky Lab eine internationale Unternehmensgruppe mit 34 Büros in 31 Ländern der Welt. Das Unternehmen beschäftigt über 3.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Programme zur Gewährleistung der IT-Sicherheit für Desktops, Laptops, Tablets, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Lösungen und Technologien für den Schutz und die Kontrolle von Arbeitsstationen und mobilen Geräten, virtuellen Maschinen, Datei- und Webservern, Mail-Gateways und Firewalls. Zum Portfolio des Unternehmens gehören ferner Spezialprodukte zum Schutz vor DDoS-Angriffen, Schutz von Umgebungen der Automatisierungstechnik und zur Verhütung von Finanzbetrug. In Verbindung mit zentralen Administrationstools bieten diese Lösungen Unternehmen beliebiger Größe die Möglichkeit, einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen und zu nutzen. 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 Hunderttausende neue Computerbedrohungen und entwickeln Mittel, um Gefahren zu erkennen und zu desinfizieren. Die Signaturen dieser Bedrohungen fließen in die Datenbanken ein, auf die die Kaspersky Lab-Programme zurückgreifen.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Software-Hersteller den Kernel von Kaspersky Anti-Virus in ihrer Software einsetzen. Zu ihnen zählen Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Lab 2014 anhand der Prüfungs- und Forschungserkenntnisse des anerkannten österreichischen Antiviren-Labors AV-Comparatives zu einem von zwei Spitzenreitern bei der Anzahl der erhaltenen Advanced+-Zertifikate gekürt. Dem Unternehmen wurde daher das Zertifikat Top Rated verliehen. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 400 Millionen Anwender. Über 270.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Seite von Kaspersky Lab:	http://www.kaspersky.com/de
Viren-Enzyklopädie:	https://de.securelist.com/
Virenlabor:	http://newvirus.kaspersky.com/de (zur Untersuchung verdächtiger Dateien und Seiten)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com/index.php?showforum=26

Zusätzlicher Schutz durch Verwendung von Kaspersky Security Network

Kaspersky Lab bietet ein zusätzliches Schutzniveau durch die Verwendung von Kaspersky Security Network. Ziel dieser Schutzmethode ist der effektive Kampf gegen komplizierte, ständig auftauchende Bedrohungen, sowie Zero-Day-Bedrohungen. Die mit Kaspersky Endpoint Security integrierten Cloud-Technologien und fachspezifische Kenntnisse der Virenanalysten von Kaspersky Lab ermöglichen einen umfangreichen Schutz gegen die kompliziertesten Bedrohungen im Netzwerk.

Weitere Informationen über den zusätzlichen Schutz von Kaspersky Endpoint Security finden Sie auf der Kaspersky-Lab-Website.

Informationen über den Code von Drittherstellern

Die Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich im Installationsordner des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Active Directory, ActiveSync, Edge, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SharePoint, SQL Server, Windows, Windows Server, Windows Phone und Windows Vista sind eingetragene Markenzeichen der Microsoft Corporation in den USA und anderen Ländern.

Android, Chrome und Google Play sind Marken von Google, Inc.

Apache und Apache feather logo sind Markenzeichen von Apache Software Foundation.

Apple, App Store, Leopard, Mac, Mac OS, macOS, Safari, Snow Leopard, OS X und Tiger sind in den USA und anderen Ländern eingetragene Warenzeichen von Apple Inc.

Cisco ist ein eingetragenes Markenzeichen von Cisco Systems, Inc und/oder seiner Partnerunternehmen in den USA und anderen Ländern.

Citrix und XenServer sind eingetragene Marken von Citrix Systems, Inc. und/oder Tochterunternehmen, und sind in den USA und anderen Ländern im Patentamt registriert.

Debian ist ein eingetragenes Warenzeichen von Software in the Public Interest, Inc.

Intel, Core, Xeon sind eingetragene Markenzeichen der Intel Corporation in den USA und anderen Ländern.

CentOS, Fedora und Red Hat Enterprise Linux sind in den USA und in anderen Ländern eingetragene Marken von Red Hat Inc.

Firefox ist ein Markenzeichen der Mozilla Foundation.

Das Logo FreeBSD ist ein eingetragenes Warenzeichen der Stiftung FreeBSD.

Oracle und Java sind eingetragene Marken der Oracle Corporation und/oder von verbundenen Unternehmen.

Linux ist ein eingetragenes Markenzeichen von Linus Torvalds in den USA und anderen Ländern.

Novell, Netware sind eingetragene Markenzeichen von Novell Inc. in den USA und anderen Ländern.

SUSE ist eine in den USA und in anderen Ländern eingetragene Marke von SUSE LLC.

Ubuntu ist eine eingetragene Marke der Canonical Ltd.

UNIX ist ein in den USA und anderen Ländern eingetragenes Markenzeichen. Die Nutzung ist durch die X/Open Company Limited lizenziert.

VMware ist ein Markenzeichen von VMware, Inc. oder eine in den USA oder anderen Ländern eingetragene Marke von VMware, Inc.

Das Markenzeichen Symbian ist Eigentum der Symbian Foundation Ltd.

BlackBerry ist eine eingetragene Marke der Research In Motion Limited in den USA. Die Marke kann auch in anderen Ländern angemeldet werden.

Sachregister

A

B

C

D

E

G

H

I

K

M

N

P

R

S

T

U

V