KASPERSKY lab

Kaspersky Security Center 10

Administratorhandbuch

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: 13.12.2016

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

Inhalt

Über dieses Dokument

Das Administratorhandbuch 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 die technische Unterstützung von Unternehmen verantwortlich sind, die Kaspersky Security Center einsetzen.

Dieses Handbuch bietet Informationen zur Konfiguration und Verwendung von Kaspersky Security Center.

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

In diesem Abschnitt

In diesem Dokument

Das Administratorhandbuch von Kaspersky Security Center enthält eine Einführung, Abschnitte, in denen die Programmoberfläche, Einstellungen, die Bedienung des Programms und die wichtigsten Aufgaben erläutert werden sowie ein Glossar zur Terminologie.

Informationsquellen über das Programm (s. S. 21)

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. 24)

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

Programmoberfläche (s. S. 47)

In diesem Abschnitt werden die wichtigsten Elemente der Benutzeroberfläche von Kaspersky Security Center sowie die Konfiguration der Benutzeroberfläche beschrieben.

Lizenzverwaltung (s. S. 64)

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

Schnellstartassistent (s. S. 75)

Dieser Abschnitt enthält Informationen zum Schnellstartassistenten für den Administrationsserver.

Grundbegriffe (s. S. 77)

Dieser Abschnitt enthält ausführliche Definitionen der Grundbegriffe zu Kaspersky Security Center.

Administrationsserver verwalten (s. S. 94)

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsservern und deren Einstellungen.

Administrationsgruppen verwalten (s. S. 109)

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsgruppen.

Remote-Administration der Programme (s. S. 118)

Dieser Abschnitt enthält Informationen über die Remote-Verwaltung der auf den Client-Geräten installierten Programme von Kaspersky Lab mithilfe von Richtlinien, Richtlinienprofilen, Aufgaben und lokalen Programmeinstellungen.

Client-Geräte verwalten (s. S. 150)

Der Abschnitt enthält Informationen über die Arbeit mit den Client-Geräten.

Berichte, Statistiken und Benachrichtigungen (s. S. 192)

Diesem Abschnitt können Sie Informationen über die Arbeit mit Berichten, Statistiken und Ereignis- und Geräteauswahlen in Kaspersky Security Center sowie über die Konfiguration der Administrationsserver-Benachrichtigungen entnehmen.

Nicht zugeordnete Geräte (s. S. 211)

Dieser Abschnitt enthält Informationen zur Arbeit mit Geräten im Firmennetzwerk, die nicht zur Administrationsgruppe gehören.

Programme auf Client-Geräten verwalten (s. S. 221)

Dieser Abschnitt beschreibt die Verwendung von Programmgruppen sowie den Vorgang für Software-Updates und die Behebung von Schwachstellen, die von Kaspersky Security Center auf Client-Geräten identifiziert werden.

Remote-Installation von Betriebssystemen und Programmen (s. S. 255)

Dieser Abschnitt beschreibt das Erstellen und die Verteilung von Betriebssystem-Abbildern auf Client-Geräten eines Netzwerks sowie die Remote-Installation von Kaspersky-Lab-Programmen und Programmen anderer Software-Hersteller.

Mobile Geräte verwalten (s. S. 267)

In diesem Abschnitt wird beschrieben, wie Sie mobile Geräte verwalten können, die mit dem Administrationsserver verbunden sind.

Self Service Portal (s. S. 315)

Dieser Abschnitt enthält Informationen über das Self Service Portal. Sie finden hier Anleitungen zur Autorisierung von Benutzern auf dem Self Service Portal, zur Erstellung von Benutzerkonten für das Self Service Portal sowie zum Hinzufügen von mobilen Geräten auf dem Self Service Portal.

Verschlüsselung und Datenschutz (s. S. 322)

Dieser Abschnitt beschreibt die Verwaltung der Datenverschlüsselung für Daten auf Festplatten von Geräten und auf Wechseldatenträgern.

Inventarisierung der im Netzwerk gefundenen Hardware (s. S. 330)

Dieser Abschnitt beschreibt die Inventur für die in das Unternehmensnetzwerk eingebundenen Geräte.

Update der Datenbanken und Programm-Module (s. S. 333)

In diesem Abschnitt werden der Download und die Verteilung von Updates für die Datenbanken und Programm-Module mithilfe von Kaspersky Security Center beschrieben.

Arbeit mit den Schlüsseln für Programme (s. S. 351)

In diesem Abschnitt werden die Möglichkeiten von Kaspersky Security Center bei der Arbeit mit Schlüsseln von Programmen beschrieben, die von Kaspersky Lab verwaltet werden.

Datenverwaltung (s. S. 357)

Dieser Abschnitt enthält Informationen zu Daten, die auf dem Administrationsserver gespeichert und zur Überwachung und Wartung von Client-Geräten verwendet werden.

Anfragen an den Technischen Support (s. S. 375)

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. 448)

In diesem Abschnitt finden Sie Informationen zum Unternehmen Kaspersky Lab.

Informationen über den Code von Drittanbietern (s. S. 450)

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. 452)

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. 375) 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-Gerät 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.

In diesem Abschnitt

Neuerungen

Neuerungen in Kaspersky Security Center gegenüber der Vorversion:

- Es ist nun möglich, Änderungen an den Einstellungen der Richtlinien, der Aufgaben und des Administrationsservers von Kaspersky Security Center zu speichern.

- Es ist nun möglich, ein Rollback der Einstellungen eines Objekts zu einer bestimmten Version des Objekts vorzunehmen (s. Abschnitt "Änderung der Richtlinie. Rollback der Änderungen" s. S. 124).
- Es ist nun möglich, den Verlauf der Revisionen anhand von Benutzer und Uhrzeit der Änderung zu filtern.
- Es ist nun möglich, den Zeitraum der Speicherung von Revisionen (standardmäßig 3 Monate) festzulegen.
- Ein Mechanismus zum Vergleichen der Revisionen von Richtlinien und Aufgaben wurde implementiert.
- Der Export der Revisionen von Richtlinien und Aufgaben in eine Textdatei wurde implementiert.
- Die Diagnostik des Vorgangs zur automatischen Installation von Patches wurde verbessert. Es wurden zusätzliche Warnungen beim Erstellen von Sicherungskopien der Daten des Administrationsservers im Installationsassistenten von Kaspersky Security Center hinzugefügt:
  - Die Wichtigkeit des Vorhandenseins von neuen Sicherungskopien der Dateien und Distributionen der vorherigen Version von Kaspersky Security Center und aller installierten Patches wird betont.
  - Es wird erklärt, was im Fall einer Update-Störung zu tun ist.
  - Es wurde eine weitere Aufforderung zur Bestätigung durch den Benutzer umgesetzt, für den Fall, dass der Benutzer keine Sicherungskopien der Daten erstellt hat.
- Der Kaspersky Security Center Administrationsagent (Windows 8/8.1, MS Surface) wird nun von Tablets mit dem Betriebssystem Windows unterstützt.
- Der Administrationsagent wurde optimiert, um die Ladezeit von Windows auf Geräten mit Kaspersky Endpoint Security für Windows und dem Administrationsagenten zu verkürzen.
- Die Ausführung des Administrationsagenten im Energiesparmodus (Standby, Ruhezustand) des Windows-Systems wurde optimiert.

- Es ist nun möglich, im Installationsassistenten von Kaspersky Security Center die aktuellen Versionen der Plug-Ins und der Installationspakete von Kaspersky Lab zu überprüfen und verfügbare Updates anzuwenden. Auch im Programmhauptfenster von Kaspersky Security Center werden verfügbare Updates für Plug-Ins, Programme und Apps bzw. Komponenten von Kaspersky Security Center angezeigt.

- Die Terminologie von Kaspersky Security Center wurde verallgemeinert und von anderen Programmen unabhängig gemacht. Beispielsweise wurde der Begriff "Computer" durch den Begriff "Gerät" ersetzt.

- Ein neuer Installationsassistent für Software-Updates wurde implementiert (s. Abschnitt "Manuelle Installation von Updates auf Geräte" s. S. 250).

- Informationen über Aufgabenausführung wurden hinzugefügt. Zur Liste mit Spalten im Fenster **Ergebnisse der Aufgabenausführung** wurden folgende Spalten hinzugefügt:

  - Indikatoren für Geräte, auf denen die Aufgabe gestartet, beendet oder mit Fehler beendet wurde.

  - Status (mit einer Beschreibung des Aufgabenstatus).

- Es ist nun möglich, dem Installationspaket manuell einen Namen zuzuweisen.

- Der Benutzer wird nun zu einer Bestätigung aufgefordert, wenn er eine Richtlinie für Kaspersky-Lab-Programme in einer Administrationsgruppe erstellt, in der bereits eine Richtlinie für das vorliegende Programm existiert.

- Im Arbeitsplatz des Ordners **Nicht zugeordnete Geräte** wurde die Schaltfläche **Regeln anpassen** hinzugefügt, um nicht zugeordnete Geräte automatisch zu verschieben (s. Abschnitt "Regeln für das automatische Verschieben von Geräten in Administrationsgruppen erstellen" s. S. 217).

- Das Kontrollkästchen **Softwareverteilungs-Assistent auf den Workstations starten** wurde zum Schnellstartassistenten hinzugefügt.

- Die Seiten des Arbeitsplatzes auf der Registerkarte **Statistik** im Knoten des Administrationsservers wurden optisch unterteilt.

- Die Navigation bei der Verwendung von Regeln für automatische Tag-Zuweisung wurde verbessert.

- Die Verwaltung des Zugriffs mithilfe von Rollen in den Eigenschaften des Administrationsservers wurde ausgearbeitet.
- Ein Filter für die Textbeschreibung des Feldes **Ereignisse** wurde hinzugefügt.
- Es ist nun möglich, Tags in den Aktivierungsregeln des Richtlinienprofils zu erstellen.
- Der schnelle Wechsel zu den Richtlinienprofilen aus dem Arbeitsplatz des Ordners **Richtlinien** und aus der Registerkarte **Richtlinien** im Knoten des Administrationsservers wurde verwirklicht.
- Es ist nun möglich, die Lage der Spalten in den Listen zu bestimmen.
- Ein Indikator für den Update-Vorgang der Installationspakete wurde hinzugefügt.
- Das Installationssymbol des Administrationsservers im Hauptfenster der Installation von Kaspersky Security Center wurde geändert.
- Die Formulierungen im Assistenten für die Konvertierung von Richtlinien und Aufgaben wurden ausgearbeitet.
- Eine Beschreibung des Schlüssels Server flags LP_ConsoleMustUsePort13291 und LP_InterUserUniqVsScope wurde hinzugefügt.
- Die Installation des iOS MDM-Servers wurde vereinfacht. Ein Installationsassistent für den iOS MDM-Server wurde implementiert.
- Die Installation von Self Service Portal wurde vereinfacht.
- Der Assistent für die Verbindung eines neuen mobilen Geräts wurde ausgearbeitet.
- Das mobile Gerät wird nach der erfolgreichen Ausführung der Befehle **Standort ermitteln** und **Tonsignal wiedergeben** (s. Abschnitt "**Befehle für die Verwaltung des Mobilgeräts**" s. S. 270).
- Der Administrator hat nun die Möglichkeit, den Status von Android-Geräten manuell auf **Kritisch** oder **Warnung** zu setzen, wenn auf solchen Geräten für die App Kaspersky Endpoint Security für Android der Zugriff auf den Dienst für erleichterte Bedienung nicht aktiviert ist, da Web-Filter in einem solchen Fall nicht ausgeführt wird.

- Die Konfiguration von Google Firebase Cloud Messaging wurde vereinfacht. Hinweise und Erklärungen wurden in die Programmoberfläche eingebaut.
- Für den iOS MDM-Server wurde ein Tool zum Verschieben von Dateien ins Backup über die Befehlszeile implementiert.
- Der Administrator von Kaspersky Security Center hat nun die Möglichkeit, das Ablaufdatum des Zertifikats für Kaspersky Security für mobile Geräte während der Ausstellung (oder der erneuten Ausstellung) des Zertifikats manuell anzugeben.
- Die Anzeige der Versionsnummer von Self Service Portal in der Benutzeroberfläche von Self Service Portal wurde umgesetzt.
- Wenn während der Installation von Kaspersky Security Center das Kontrollkästchen **Unterstützung für mobile Geräte** aktiviert war, werden alle notwendigen Einstellungen der Funktionalität zur Verwaltung von mobilen Geräten und von Kaspersky Security für mobile Geräte im Schnellstartassistenten von Kaspersky Security Center vorgenommen.
- Das Design der Funktionalität zur Verwaltung von Patches und Updates wurde ausgearbeitet.
- Die Komponente Verwaltung von Schwachstellen und Patches wurde ausgearbeitet.
- Das Monitoring und die Schwachstellensuche wurden erweitert.
- Die Kontrolle ausgeführter Aufgaben wurde erweitert.
- Die Weitergabe von Ereignissen im Format Syslog (RFC 5424) an SIEM-Systeme wurde umgesetzt (s. Abschnitt "Export von Ereignissen in das SIEM-System" s. S. 204).
- Die Hardware-Typen in der Benutzeroberfläche von Kaspersky Security Center wurden vereinheitlicht.
- Die Informationen über die Ergebnisse der Ausführung der Aufgaben **Erforderliche Updates installieren und Schwachstellen schließen** und **Nach Schwachstellen und erforderlichen Updates suchen** wurden ergänzt.
- Eine zusätzliche Überprüfung vor dem Start der Aufgabe **Installationspaket anhand des Betriebssystem-Images des Mustergeräts erstellen** wurde implementiert.

Dabei wird geprüft, ob das Benutzerkonto, das vom Administrator angegeben wurde, über Schreibrechte für den angegebenen freigegebenen Ordner verfügt, in dem das Image temporär gespeichert werden soll.

- Es wird nun automatisch ein Vorfall erstellt, wenn auf dem Gerät, das die Rolle des Update-Agenten übernimmt, kein freier Speicherplatz mehr verfügbar ist (s. Abschnitt "Update-Agent" s. S. 90).

Lieferumfang

Sie können das Programm über den Online-Shop von Kaspersky Lab (beispielsweise http://www.kaspersky.com/de/, Abschnitt **Online-Shop**) oder bei unseren Vertriebspartnern erwerben.

Beim Kauf von Kaspersky Security Center in einem Online-Shop kopieren Sie das Programm von der Seite des Online-Shops. Sie erhalten die zur Programmaktivierung erforderlichen Informationen nach Eingang des Rechnungsbetrags per E-Mail.

Ausführliche Informationen zum Kauf und Lieferumfang erhalten Sie bei unserer Vertriebsabteilung.

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.

Programmoberfläche

In diesem Abschnitt werden die wichtigsten Elemente der Benutzeroberfläche von Kaspersky Security Center sowie die Konfiguration der Benutzeroberfläche beschrieben.

Das Anzeigen, Erstellen, Ändern und Konfigurieren der Administrationsgruppen sowie die zentrale Verwaltung der auf den Client-Geräten installierten Kaspersky-Lab-Programme erfolgen vom Administrator-Arbeitsplatz aus. Die Administrationsschnittstelle stellt die Komponente Verwaltungskonsole zur Verfügung. Sie ist ein spezielles, autonomes Snap-In, das in die Microsoft Management Console (MMC) integriert wird. Demzufolge ist die Benutzeroberfläche von Kaspersky Security Center Standard für die MMC.

Die Verwaltungskonsole ermöglicht das Herstellen einer Verbindung mit dem Remote-Administrationsserver über das Internet.

Für die lokale Arbeit mit Client-Geräten bietet das Programm die Möglichkeit, mit dem Windows-Standardprogramm Remotedesktopverbindung eine Remote-Verbindung zum Computer über die Verwaltungskonsole einzurichten.

Dafür muss auf dem Client-Gerät eine Remotedesktopverbindung zugelassen sein.

In diesem Abschnitt

Programmhauptfenster

Das Programmhauptfenster (s. Abb. unten) besteht aus einem Menü, einer Symbolleiste, einer Konsolenstruktur und einem Arbeitsplatz. Das Menü ermöglicht die Verwaltung der Fenster und den Zugriff auf das Hilfesystem. Das Menü **Aktion** enthält die gleichen Befehle wie das Kontextmenü für das aktuelle Objekt der Konsolenstruktur.

Die Schaltflächen der Symbolleiste gewährleisten den direkten Zugriff auf einige Menüpunkte. Die Auswahl der Schaltflächen hängt von dem in der Konsolenstruktur ausgewählten Knoten oder Ordner ab.

Die Ansicht des Arbeitsplatzes des Hauptfensters hängt davon ab, zu welchem Knoten (Ordner) der Konsolenstruktur der Arbeitsplatz gehört und welche Funktionen er ausführt.

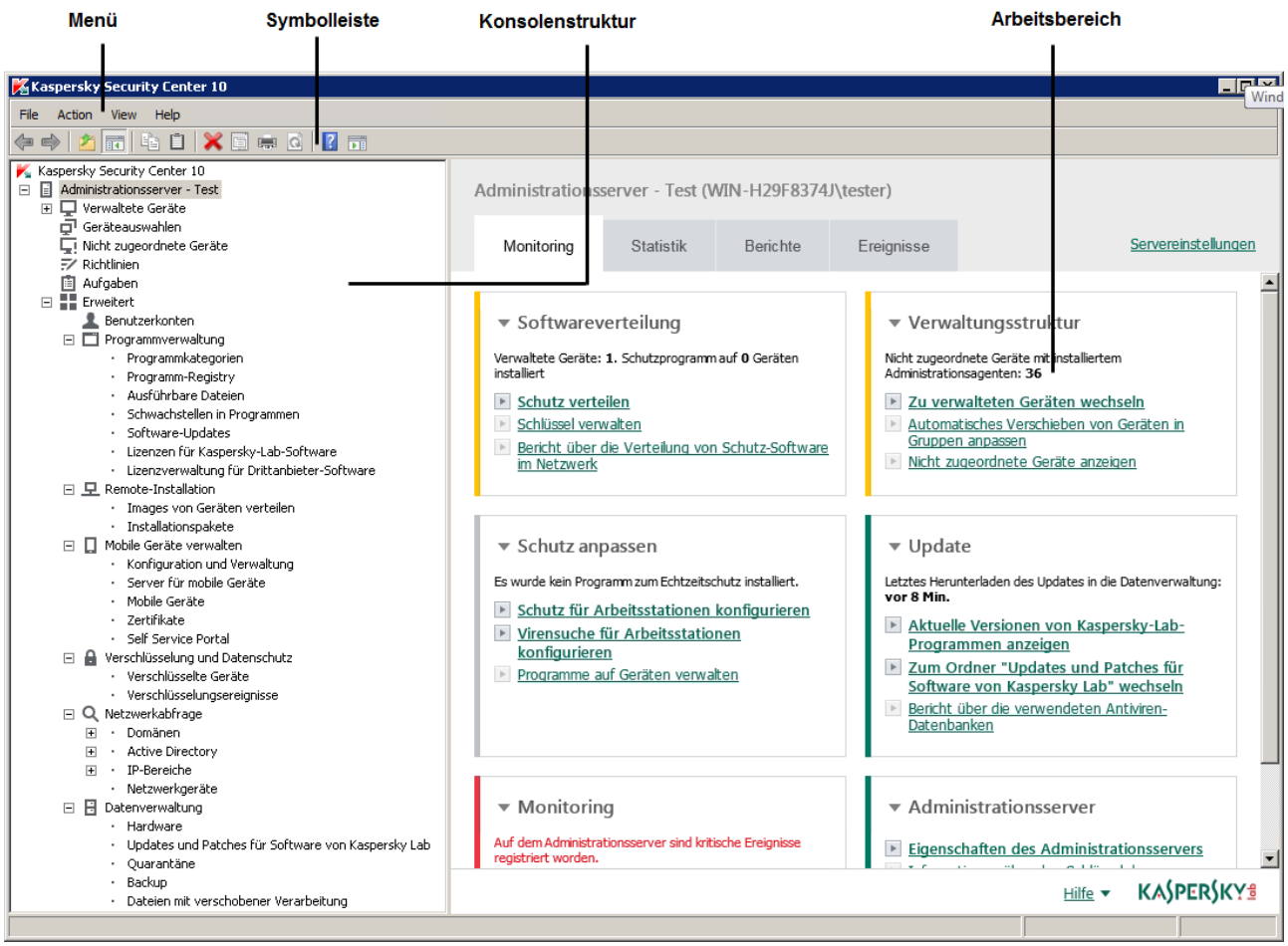


Abbildung 1. Programmhauptfenster von Kaspersky Security Center

Konsolenstruktur

Die Konsolenstruktur (s. Abb. unten) dient zur Anzeige der im Netzwerk angelegten Hierarchie der Administrationsserver, der Struktur ihrer Administrationsgruppen sowie anderer Objekte des Programms (z. B. Ordner **Datenverwaltung** und **Programmverwaltung**).
Die Namensumgebung von Kaspersky Security Center kann mehrere Knoten mit Namen von Servern enthalten, die die Netzwerkstruktur der Administrationsserver widerspiegeln.

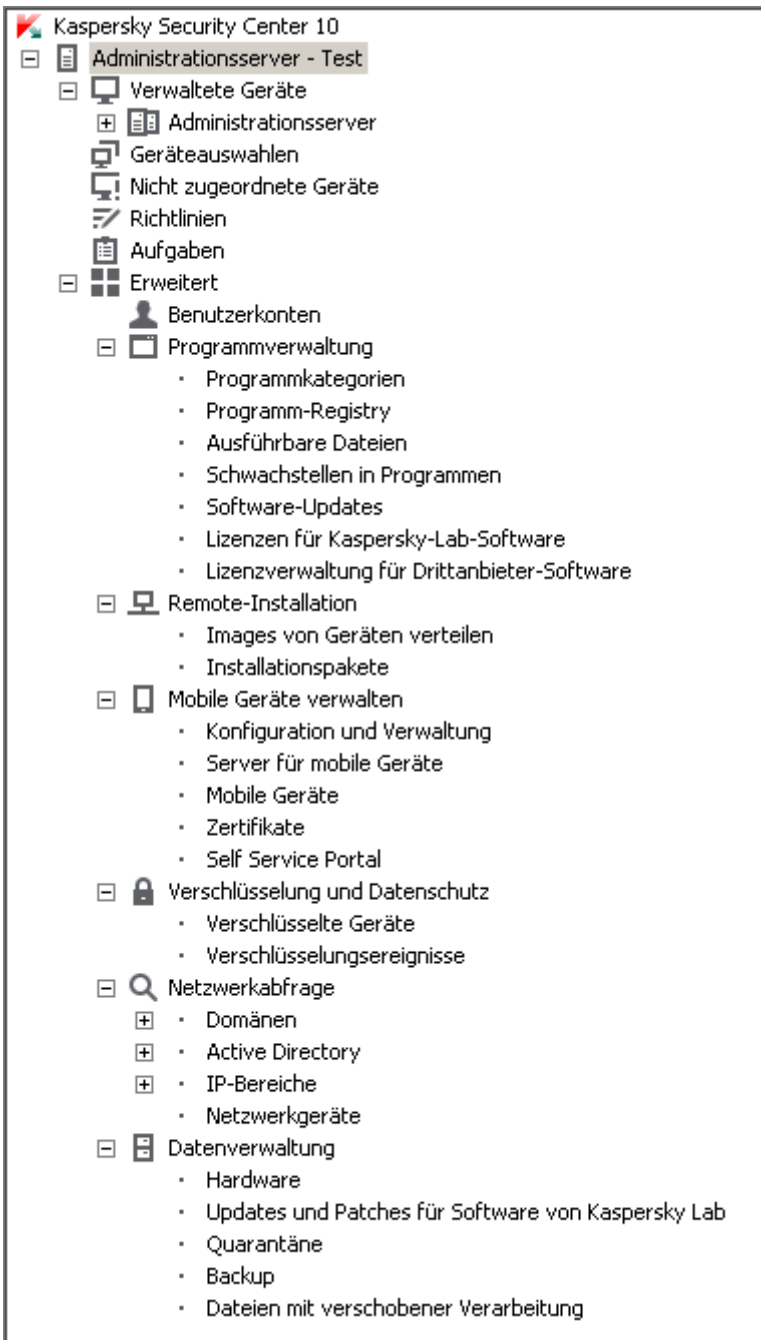


Abbildung 2. Konsolenstruktur

Knoten Administrationsserver

Der Knoten **Administrationsserver – <Gerätename>** ist ein Container, der die Struktur des angegebenen Administrationsservers darstellt.

Der Arbeitsplatz des Knotens **Administrationsserver** enthält eine Übersicht über den aktuellen Status des Programms und der Geräte, die sich unter der Verwaltung des Administrationsservers befinden. Die Informationen im Arbeitsplatz sind auf Registerkarten verteilt:

- **Monitoring**. Auf der Registerkarte **Monitoring** werden in Echtzeit Informationen über die Ausführung des Programms und den aktuellen Status der Client-Geräte angezeigt. Wichtige Nachrichten für den Administrator (beispielsweise Nachrichten über Schwachstellen, Fehler, erkannte Viren) werden farbig hervorgehoben. Mithilfe der Links auf der Registerkarte **Monitoring** können Sie typische Administratoraufgaben ausführen (z. B. ein Schutzprogramm auf Client-Geräten installieren und konfigurieren) und zu anderen Ordnern der Konsolenstruktur wechseln.

- **Statistik**. Enthält eine Auswahl von Diagrammen, die nach Themen (Schutzstatus, Antiviren-Statistik, Updates und andere) gruppiert sind. In den Diagrammen werden aktuelle Informationen über die Ausführung des Programms und den Zustand der Client-Geräte in grafischer Form dargestellt.

- **Berichte**. Enthält Vorlagen für die Berichte, die vom Programm erstellt werden. Auf dieser Registerkarte können Sie Berichte aus den vordefinierten Vorlagen erstellen sowie eigene Berichtsvorlagen erstellen.

- **Ereignisse**. Enthält Einträge über Ereignisse, die während der Ausführung des Programms registriert wurden. Zur besseren Lesbarkeit und Sortierung, werden die Einträge thematisch unterteilt. Auf dieser Registerkarte können Sie eine automatisch erstelle Ereignisauswahl anzeigen sowie Ihre eigenen Auswahlen erstellen.

Ordner im Knoten Administrationsserver

Der Knoten **Administrationsserver – <Gerätename>** enthält die folgenden Ordner:

- **Verwaltete Geräte** Der Ordner Verwaltete Geräte dient zum Speichern, Darstellen, Konfigurieren und Ändern der Struktur von Administrationsgruppen, von Gruppenrichtlinien und von Gruppenaufgaben.
- **Geräteauswahlen** Der Ordner dient zur schnellen Auswahl von Geräten, die bestimmten Kriterien entsprechen (Geräteauswahlen), aus der Gesamtheit der verwalteten Geräte. Beispielsweise können Sie schnell Geräte auswählen, auf denen kein Schutzprogramm installiert ist, und zu diesen Geräten wechseln (ihre Liste anzeigen). Mit den ausgewählten Geräten können Aktionen ausgeführt werden, beispielsweise können ihnen Aufgaben zugewiesen werden. Sie können vordefinierte Auswahlen verwenden oder Ihre eigenen (benutzerdefinierten) Auswahlen erstellen.
- **Nicht zugeordnete Geräte**. Dieser Ordner enthält eine Liste der Geräte, die keiner Administrationsgruppe angehören. Sie können mit den nicht zugeordneten Geräten Aktionen ausführen: sie in Administrationsgruppen verschieben oder Programme darauf installieren.
- **Richtlinien** Dieser Ordner ist zur Anzeige und Erstellung von Richtlinien vorgesehen.
- **Aufgaben**. Dieser Ordner ist zur Anzeige und Erstellung von Aufgaben vorgesehen.
- **Erweitert**. Dieser Ordner enthält eine Reihe von Unterordnern, die den verschiedenen Funktionsgruppen des Programms entsprechen.

Ordner Erweitert. Ordner in der Konsolenstruktur verschieben

Zum Ordner **Erweitert** gehören folgende Unterordner:

- **Benutzerkonten** Dieser Ordner enthält eine Liste der Benutzerkonten des Netzwerks.
- **Programmverwaltung** Dieser Ordner dient der Verwaltung der auf den Netzwerkgeräten installierten Programme. Der Ordner **Programmverwaltung** enthält folgende Unterordner:

- **Programmkategorien**. Der Ordner dient dazu, mit Programmkategorien zu arbeiten.
- **Programm-Registry**. Enthält eine Liste von Programmen auf den Geräten mit installiertem Administrationsagenten.
- **Ausführbare Dateien**. Enthält eine Liste ausführbarer Dateien, die sich auf den Client-Geräten mit installiertem Administrationsagenten befinden.
- **Schwachstellen in Programmen**. Enthält eine Liste mit Schwachstellen in Programmen auf den Geräten mit installiertem Administrationsagenten.
- **Software-Updates**. Enthält eine Liste der vom Administrationsserver empfangenen Programm-Updates, die auf die Geräte verteilt werden können.
- **Lizenzen für Kaspersky Lab-Software**. Enthält eine Liste der verfügbaren Schlüssel für Kaspersky Lab-Programme. Im Arbeitsplatz des Ordners können Sie neue Schlüssel in den Schlüsselspeicher hinzufügen, Schlüssel auf die verwalteten Geräte verteilen oder einen Bericht über die Schlüsselnutzung anzeigen.
- **Lizenzverwaltung für Drittanbieter-Software**. Enthält eine Liste der lizenzierten Programmgruppen. Mithilfe von lizenzierten Programmgruppen kann die Nutzung von Lizenzen für Programme von Drittherstellern (Programme, die nicht von Kaspersky Lab stammen) und die Verletzung der Lizenzbeschränkungen verfolgt werden.

- **Remote-Installation** Dieser Ordner dient zur Verwaltung der Remote-Installationen von Betriebssystemen und Programmen. Der Ordner **Remote-Installation** enthält folgende Unterordner:
  - **Images von Geräten verteilen**. Der Ordner dient der Verteilung von Betriebssystem-Abbildern auf die Geräte.
  - **Installationspakete**. Dieser Ordner enthält eine Liste der Installationspakete, die zur Remote-Installation von Programmen auf den Client-Geräten verwendet werden können.
- **Mobile Geräte verwalten** Dieser Ordner dient zur Verwaltung der mobilen Geräte. Der Ordner **Mobile Geräte verwalten** enthält folgenden Unterordner:

- **Mobile Geräte** Dient zur Verwaltung von mobilen KES-Geräten, Exchange ActiveSync-Mobilgeräten und mobilen iOS MDM-Geräten.

- **Zertifikate**. Dient zur Verwaltung von Zertifikaten für mobile Geräte.

- **Verschlüsselung und Datenschutz** Dieser Ordner wird zur Verwaltung der Datenverschlüsselung auf Festplatten und Wechseldatenträgern verwendet.

- **Netzwerkabfrage**. Dieser Ordner zeigt das Netzwerk an, in dem der Administrationsserver installiert ist. Der Administrationsserver empfängt Daten über die Netzwerkstruktur und deren Geräte, indem das Windows-Netzwerk, die IP-Bereiche und das Active Directory® im Unternehmensnetzwerk regelmäßig durchsucht werden. Die Suchergebnisse werden in den Arbeitsplätzen der entsprechenden Ordner **Domänen**, **IP-Bereiche** und **Active Directory** angezeigt.

- **Datenverwaltung** Dieser Ordner dient der Arbeit mit Objekten, die zur Überwachung des Status der Geräte und für deren Bearbeitung verwendet werden. Der Ordner **Datenverwaltung** enthält folgende Unterordner:

  - **Updates und Patches für Software von Kaspersky Lab**. Enthält eine Liste der vom Administrationsserver empfangenen Updates, die auf die Geräte verteilt werden können.

  - **Hardware**. Der Ordner enthält eine Liste der im Unternehmensnetzwerk angeschlossenen Hardware.

  - **Quarantäne**. Der Ordner enthält eine Liste der Objekte, die von Antiviren-Programmen in die Quarantäne-Ordner auf den Geräten verschoben wurden.

  - **Backup**. Dieser Ordner enthält eine Liste der Backup-Kopien von Dateien, die während der Desinfizierung auf den Geräten gelöscht oder verändert wurden.

  - **Dateien mit verschobener Verarbeitung**. Der Ordner enthält eine Liste der Dateien, für die von Antiviren-Programmen die Notwendigkeit einer verschobenen Desinfizierung bestimmt wurde.

Sie können die Auswahl der Unterordner des Ordners **Erweitert** verändern. Unterordner, die aktiv verwendet werden, können aus dem Ordner **Erweitert** auf eine höhere Ebene verschoben werden. Ordner, die nur selten verwendet werden, können in den Ordner **Erweitert** verschoben werden.

*Gehen Sie folgendermaßen vor, um einen Unterordner aus dem Ordner **Erweitert** herauszuziehen:*

1. Wählen Sie in der Konsolenstruktur den Unterordner aus, den Sie aus dem Ordner **Erweitert** verschieben möchten.

2. Wählen Sie im Kontextmenü des Unterordners den Punkt **Ansicht** → **Verschieben aus dem Ordner Erweitert**.

> Sie können einen Unterordner im Arbeitsplatz des Ordners **Erweitert** im Block mit dem Namen des Unterordners aus dem Ordner **Erweitert** auch mithilfe des Links **Verschieben aus dem Ordner Erweitert** verschieben.

*Gehen Sie folgendermaßen vor, um einen Ordner in den Ordner **Erweitert** zu verschieben:*

1. Wählen Sie in der Konsolenstruktur den Ordner aus, der in den Ordner **Erweitert** verschoben werden soll.

2. Wählen Sie im Kontextmenü des Ordners den Punkt **Ansicht** → **In den Ordner Erweitert verschieben**.

Arbeitsplatz

Der Arbeitsplatz (s. Abb. unten) enthält folgende Elemente:

- Listen von Objekten, die vom Administrator mithilfe des Programms verwaltet werden (Geräte, Administrationsgruppen, Benutzerkonten, Richtlinien, Aufgaben, Einträge über Ereignisse,andere Programme etc.) (s. Abschnitt "Elemente des Arbeitsplatzes" auf S. 56);

- Verwaltungselemente (Schaltflächen, Dropdown-Listen mit Befehlen, Links zur Ausführung von Befehlen und zum Wechseln zu anderen Ordnern der Konsolenstruktur);

- Informationen in textlicher und grafischer Form (Nachrichten des Programms, Diagramme in Informationsbereichen, statistische und hilfreiche Informationen) (s. Abschnitt "Informationsblöcke" auf S. 57).

Der Inhalt des Arbeitsplatzes entspricht dem Knoten oder Ordner, der in der Konsolenstruktur ausgewählt ist.

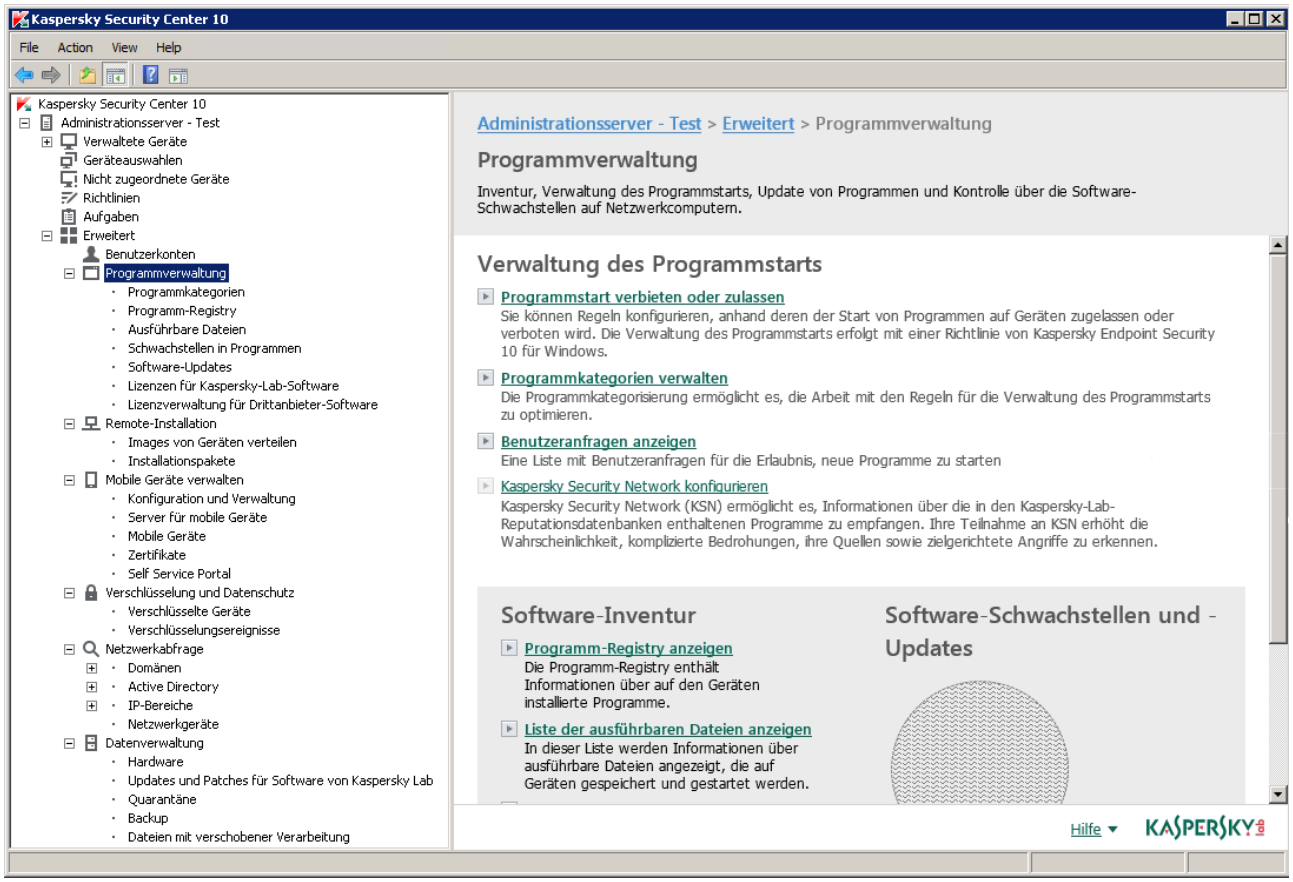


Abbildung 3. Arbeitsplatz

Der Arbeitsplatz eines Knotens oder Ordners kann mehrere Registerkarten enthalten (s. Abb. unten): Jede Registerkarte entspricht einer bestimmen Gruppe (einem Typ) von Objekten oder Funktionen des Programms.

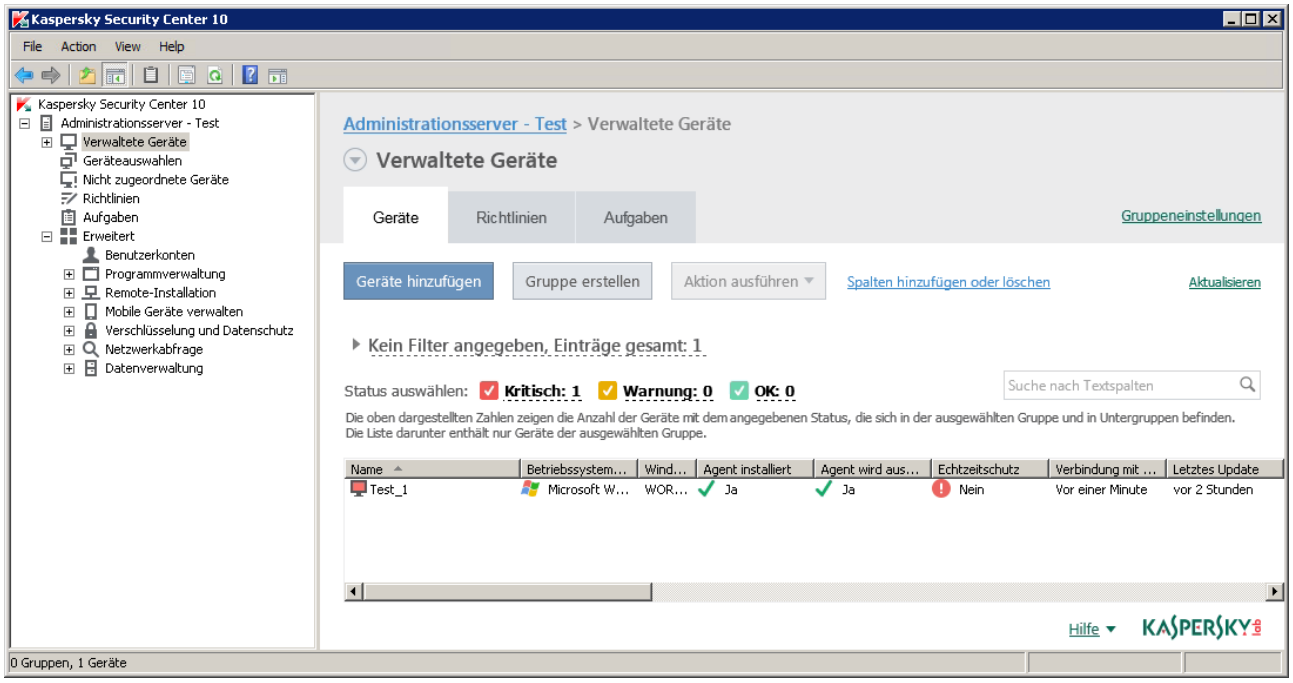


Abbildung 4. Arbeitsplatz, der in Registerkarten unterteilt ist

In diesem Abschnitt

Elemente des Arbeitsplatzes

Der Arbeitsplatz eines Ordners oder Knotens kann folgende Elemente enthalten (s. Abb. unten):

- Block zur Verwaltung der Liste. Enthält Schaltflächen, Dropdown-Listen für Befehle und Links. Dient zur Ausführung von Aktionen mit den in der Liste ausgewählten Objekten.
- Objektliste. Enthält Verwaltungsobjekte (z. B. Geräte, Benutzerkonten, Richtlinien, Aufgaben). Sie können die Objekte mithilfe des Verwaltungsblocks und den Befehlen aus dem Kontextmenü eines Objekts in der Liste sortieren und filtern sowie Aktionen mit

ihnen ausführen. Darüber hinaus können Sie die Auswahl der in der Liste angezeigten Spalten anpassen.

- Block zur Bearbeitung eines ausgewählten Objekts. Enthält eine Übersicht des ausgewählten Objekts. Dieser Block kann auch Links für rasche Aktionen mit dem ausgewählten Objekt enthalten. Beispielsweise enthält der Block zur Bearbeitung einer ausgewählten Richtlinie einen Link zum Konfigurationsfenster der Richtlinie.

- Block zur Datenfilterung. Mithilfe des Blocks zur Datenfilterung können Sie die Darstellung der Objekte in der Liste anpassen. Beispielsweise kann mithilfe des Blocks zur Datenfilterung die Geräteliste so angepasst werden, dass in ihr nur Geräte mit dem Status "Kritisch" angezeigt werden.

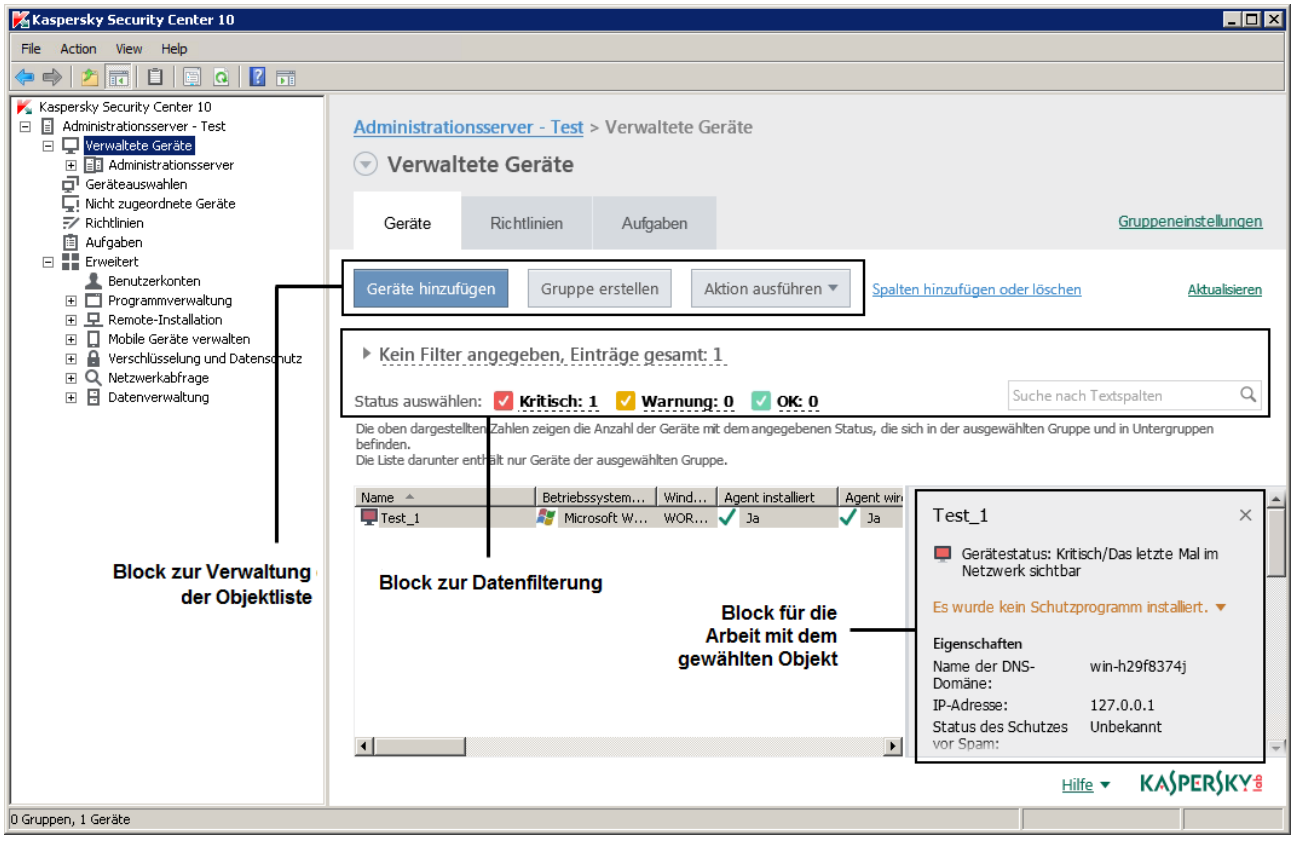


Abbildung 5. Informationsbereich, in dem Verwaltungsobjekte dargestellt sind

Informationsblöcke

Im Arbeitsplatz des Knotens **Administrationsserver** werden auf der Registerkarte **Statistik** in Informationsbereichen statistische Daten angezeigt. Die Informationsbereiche sind auf mehrere thematische Seiten aufgeteilt (s. Abb. unten). Sie können die Darstellung der Daten

in den Informationsbereichen anpassen: Diagrammtyp und Datenauswahl ändern, Informationsbereiche ändern und hinzufügen sowie ganze Seiten zur Registerkarte **Statistik** hinzufügen (s. Abschnitt "**Statistik**" auf S. 196).

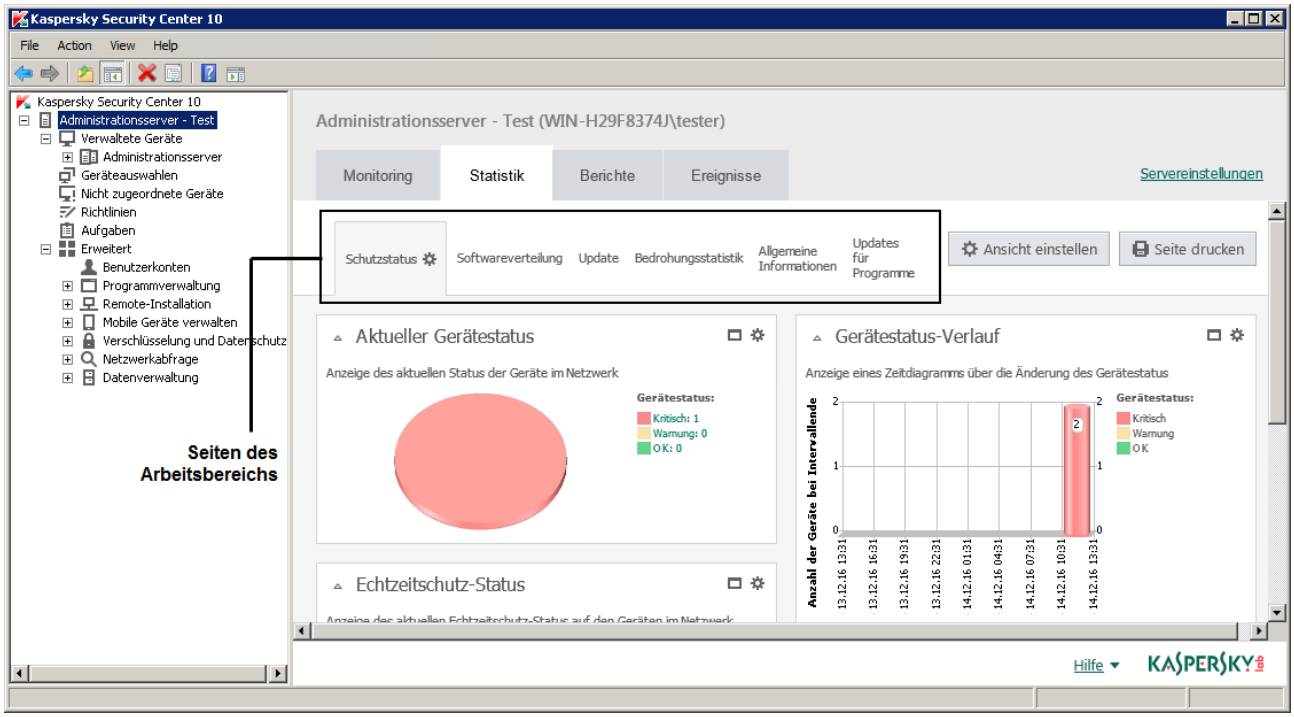
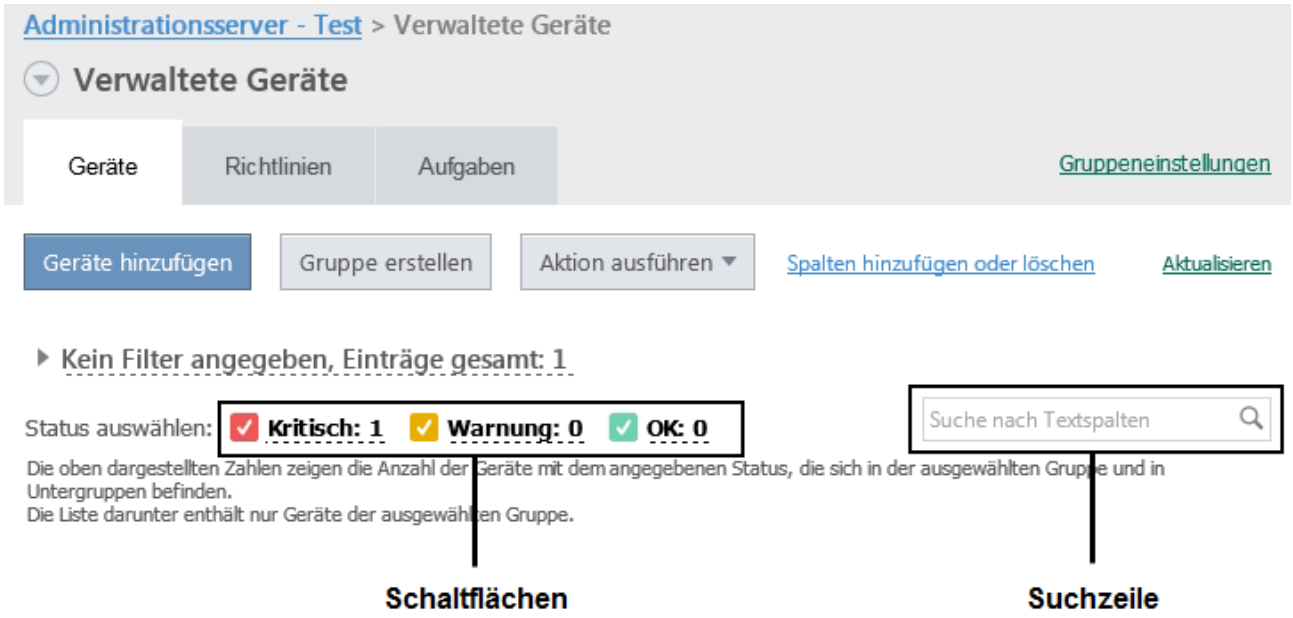


Abbildung 6. Arbeitsplatz, der in Seiten unterteilt ist

Block zur Datenfilterung

Der *Block zur Datenfilterung* (im Folgenden *Filterblock* genannt) wird in den Arbeitsplätzen und Abschnitten der Dialogfenster verwendet, die Listen mit Objekten enthalten (z. B. Geräte, Programme, Schwachstellen, Benutzer).

Der Filterblock kann eine Suchzeile, einen Filter und Schaltflächen enthalten (s. Abb. unten).



Erweiterter Filterblock**. Filtereinstellungen**

Zum Filtern von Daten können Sie den Standardblock oder den erweiterten Filterblock verwenden (s. Abb. unten). Im Standard-Filterblock können Sie Daten mithilfe der Suchzeile und der Schaltflächen im Block **Status auswählen** filtern. Im erweiterten Filterblock stehen Ihnen zusätzliche Filterkriterien zur Verfügung. Die zusätzlichen Kriterien können über den Link **Filter anpassen** aufgerufen werden.

Um die Filterung anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie auf den Bereich **Kein Filter angegeben**.

   Im rechten Teil des Fensters wird der Link **Filter anpassen** angezeigt.

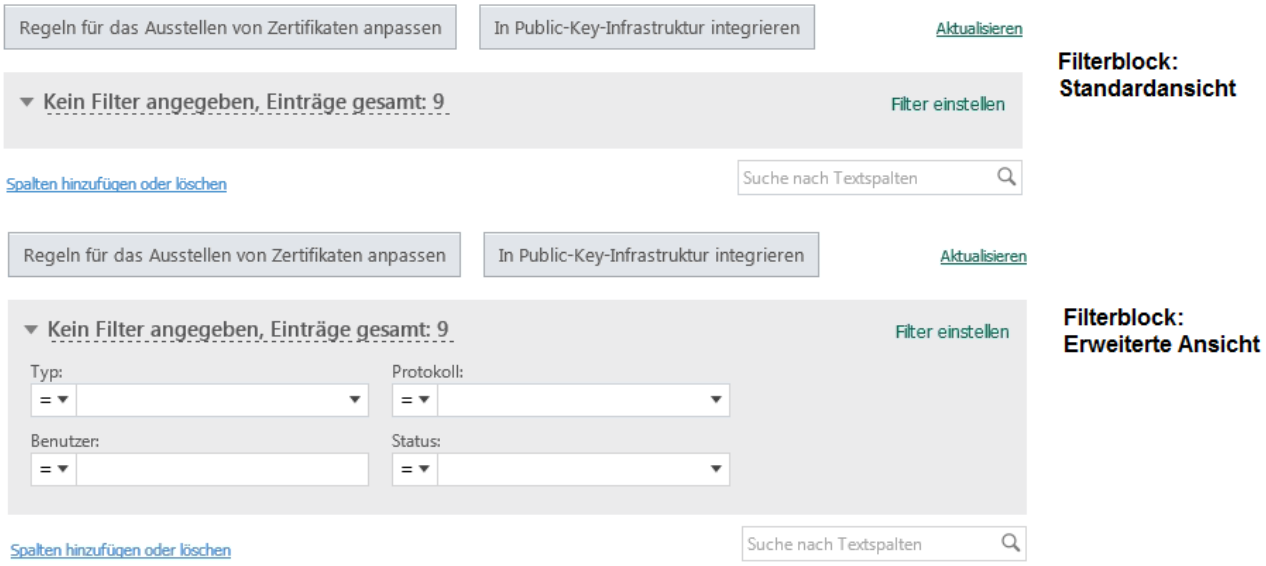
2. Wählen Sie über den Link **Filter anpassen** die Filterkriterien aus.

   Die gewählten Kriterien erscheinen auf grauem Hintergrund im Feld **Filter**.

3. Geben Sie für jedes Kriterium einen Wert an (z. B. "*Agent installiert*").

4. Konfigurieren Sie im Block **Status auswählen** die zusätzliche Filterung der Geräte anhand von Status (*Kritisch*, *Warnung*, *OK*).

Dem Filter entsprechende Geräte werden in einer Liste angezeigt. Sie können auch Geräte nach Schlüsselwörtern und egulären Ausdrücken (s. Abschnitt "Neuerungen" auf S. 25) im Feld **Suchen** suchen.



Kontextmenü

Jedes Objekt in der Kaspersky Security Center Konsolenstruktur verfügt über ein Kontextmenü. Neben den Standardbefehlen des Kontextmenüs der Microsoft Management Console befinden sich dort zusätzliche Befehle, mit denen dieses Objekt bearbeitet werden kann. Eine Auflistung der zusätzlichen Befehle des Kontextmenüs entsprechend den verschiedenen Objekten der Konsolenstruktur finden Sie in den Anhängen (s. Abschnitt "Befehle des Kontextmenüs" auf S. 415).

Einige Objekte im Arbeitsplatz (z. B. Geräte in der Liste der verwalteten Geräte, andere Objekte in Listen) verfügen ebenfalls über ein Kontextmenü mit zusätzlichen Befehlen.

Benutzeroberfläche anpassen

Sie können die Benutzeroberfläche von Kaspersky Security Center anpassen:

- Objekte in der Konsolenstruktur, den Arbeitsplätzen, Eigenschaften von Objekten (Ordner, Abschnitte) in Abhängigkeit der verwendeten Funktionen anzeigen und ausblenden.
- Teile des Hauptfensters (beispielsweise Konsolenstruktur, Standardmenüs **Aktionen** und **Ansicht**) anzeigen und ausblenden.

Um die Benutzeroberfläche von Kaspersky Security Center abhängig von den verwendeten Funktionen anzupassen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Wählen Sie im Programmfenster den Punkt **Ansicht** → **Benutzeroberfläche anpassen**.
3. Konfigurieren Sie im geöffneten Fenster **Benutzeroberfläche anpassen** die Anzeige der Oberflächenelemente. Verwenden Sie dazu die folgenden Kontrollkästchen:

   - **Systems Management anzeigen.**

     Wenn dieses Kontrollkästchen aktiviert ist, wird im Ordner **Remote-Installation** der Unterordner **Images von Geräten verteilen** und im Ordner **Datenverwaltung** der Unterordner **Hardware** angezeigt.

     Dieses Kontrollkästchen ist standardmäßig deaktiviert.

   - **Verschlüsselung anzeigen.**

     Ist das Kontrollkästchen aktiviert, ist die Verwaltung der Datenverschlüsselung auf Geräten verfügbar, die mit dem Netzwerk verbunden werden. Nach einem Neustart des Programms wird in der Konsolenstruktur der Ordner **Verschlüsselung und Datenschutz** angezeigt.

     Dieses Kontrollkästchen ist standardmäßig deaktiviert.

- **Einstellungen für die Arbeitsplatz-Überwachung anzeigen.**

  Ist das Kontrollkästchen aktiviert, werden im Abschnitt **Arbeitsplatz-Überwachung** des Eigenschaftenfensters der Kaspersky Endpoint Security 10 für Windows Richtlinie die folgenden Abschnitte angezeigt:

- **Kontrolle des Programmstarts.**
- **Überwachung von Schwachstellen.**
- **Gerätekontrolle.**
- **Web-Kontrolle.**

  Ist das Kontrollkästchen deaktiviert, werden die oben angegebenen Abschnitte im Abschnitt **Arbeitsplatz-Überwachung** nicht angezeigt.

  Dieses Kontrollkästchen ist standardmäßig deaktiviert.

- **Verwaltung von mobilen Geräten anzeigen.**

  Ist das Kontrollkästchen aktiviert, ist die Funktion **Mobile Geräte verwalten** verfügbar. Nach einem Neustart des Programms wird in der Konsolenstruktur der Ordner **Mobile Geräte** angezeigt.

  Dieses Kontrollkästchen ist standardmäßig deaktiviert.

- **Untergeordnete Administrationsserver anzeigen.**

  Ist das Kontrollkästchen aktiviert, werden in der Konsolenstruktur Knoten für untergeordnete und virtuelle Administrationsserver in den Administrationsgruppen angezeigt. Dabei sind Funktionen verfügbar, die sich auf untergeordnete und virtuelle Administrationsserver beziehen (Beispiel: Erstellung von Aufgaben zur Remote-Installation von Programmen auf untergeordneten Administrationsservern).

  Dieses Kontrollkästchen ist standardmäßig aktiviert.

- **Abschnitte mit Sicherheitseinstellungen anzeigen.**

  Wenn Sie das Kontrollkästchen aktivieren, wird in den Eigenschaftenfenstern des Administrationsservers, der Administrationsgruppen und anderer Objekte der Abschnitt **Sicherheit** angezeigt. Dadurch können Sie Benutzern und Benutzergruppen Rechte für Objekte zuweisen, die sich von Standardrechten unterscheiden.

  Dieses Kontrollkästchen ist standardmäßig aktiviert.

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

Um mehrere Änderungen anzuwenden, muss das Programmhauptfenster geschlossen und wieder geöffnet werden.

Um die Darstellung von Elementen des Programmhauptfensters anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Menü des Programmfensters den Punkt **Ansicht** → **Anpassen**.
2. Passen Sie im folgenden Fenster **Ansicht anpassen** die Darstellung der Elemente des Hauptfensters mithilfe der Kontrollkästchen an.
3. Klicken Sie auf die Schaltfläche **OK**.

Lizenzverwaltung

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

In diesem Abschnitt

Über den Lizenzvertrag

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

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

Sie haben folgende Möglichkeiten, sich mit den Bedingungen des Lizenzvertrags vertraut zu machen:

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

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

Über die Lizenz

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

Die Lizenz gewährt Ihnen das Recht, die folgenden Dienstleistungen zu benutzen:

- Nutzung des Programms gemäß den Bestimmungen des Lizenzvertrages
- Technischer Support.

Der Umfang der gebotenen Dienstleistungen sowie die Nutzungsdauer des Programms hängen vom Typ der Lizenz ab, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Test* – eine kostenlose Lizenz zum Kennenlernen des Programms.

  Eine Testlizenz verfügt in der Regel über eine kurze Gültigkeitsdauer. Nach Ablauf der Testlizenz stellt Kaspersky Security Center die Funktion ein. Um das Programm weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

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

- *Kommerziell* – eine kostenpflichtige Lizenz, die beim Kauf des Programms zur Verfügung gestellt wird.

Nach Ablauf der Gültigkeitsdauer der kommerziellen Lizenz setzt das Programm seine Arbeit mit eingeschränkter Funktionalität fort (z. B. sind kein Datenbanken-Update und keine Nutzung des Dienstes Kaspersky Security Center möglich). Zur weiteren Nutzung von Kaspersky Security Center mit allen Funktionen müssen Sie die Gültigkeitsdauer der kommerziellen Lizenz verlängern.

Es wird empfohlen, die Gültigkeitsdauer einer Lizenz spätestens zum Ablaufdatum der aktiven Lizenz zu verlängern, um einen optimalen Schutz zu gewährleisten.

Über das Lizenzzertifikat

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

Das Lizenzzertifikat enthält folgende Informationen über die ausgestellte Lizenz:

- Bestellnummer
- Informationen über den Benutzer, dem die Lizenz ausgestellt wird
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- Quantitative Einschränkungen im Hinblick auf die Lizenzierungseinheiten (beispielsweise Geräte, auf denen das Programm mit dieser Lizenz verwendet werden darf)
- Datum, an dem die Gültigkeitsdauer der Lizenz beginnt
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp.

Über den Schlüssel

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

Sie können einen Schlüssel mithilfe einer der folgenden Methoden zum Programm hinzufügen: *Schlüsseldatei* anwenden oder *Aktivierungscode* eingeben. Nachdem Sie den Schlüssel im Programm hinzugefügt haben, wird er auf der Programmoberfläche als eindeutige Folge aus Buchstaben und Ziffern angezeigt.

Ein Schlüssel kann von Kaspersky Lab gesperrt werden, falls die Bedingungen des Lizenzvertrags verletzt werden. Wenn ein Schlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um das Programm zu nutzen.

Es gibt einen aktiven Schlüssel und einen Reserveschlüssel.

Aktiver Schlüssel – Schlüssel, der im Augenblick für die Programmausführung verwendet wird. Als aktiver Schlüssel kann ein Schlüssel für eine Testlizenz oder für eine kommerzielle Lizenz hinzugefügt werden. Im Programm kann jeweils nur ein aktiver Schlüssel installiert werden.

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

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

Lizenzierungsvarianten für Kaspersky Security Center

Im Programm Kaspersky Security Center kann die Lizenz für verschiedene Gruppen von Funktionen verteilt werden.

Basisfunktionen der Administrationskonsole

Es stehen folgende Funktionen zur Verfügung:

- virtuelle Administrationsserver erstellen, um ein Netzwerk entfernter Standorte bzw. Kundenunternehmen zu verwalten
- Hierarchie der Administrationsgruppen erstellen, um eine Gruppe von bestimmten Geräten als Ganzes zu verwalten

- Status der Antiviren-Sicherheit eines Unternehmens kontrollieren
- Remote-Installation von Programmen
- Liste der Betriebssystem-Abbilder anzeigen, die für die Remote-Installation verfügbar sind
- Einstellungen der auf den Client-Geräten installierten Programme zentral anpassen
- vorhandene lizenzierte Programmgruppen anzeigen und ändern
- Statistiken und Berichte über die Ausführung von Programmen sowie Benachrichtigungen über kritische Ereignisse erhalten
- Verschlüsselung und Datenschutz verwalten
- Liste der durch eine Netzwerkabfrage gefundenen Geräte anzeigen und manuell bearbeiten
- zentral Dateien verwalten, die in die Quarantäne, ins Backup oder in die Ablage für Dateien mit verschobener Verarbeitung verschoben wurden.

Das Programm Kaspersky Security Center, das die Basisfunktionen der Administrationskonsole unterstützt, wird zusammen mit den Kaspersky-Lab-Produkten geliefert, die für den Schutz des Unternehmensnetzwerks konzipiert sind. Außerdem steht es auf der Kaspersky Lab-Webseite zum Download bereit (http://www.kaspersky.com/de/).

Vor der Aktivierung des Programms oder vor dem Ablauf der kommerziellen Lizenz wird Kaspersky Security Center im Modus Basisfunktionen der Administrationskonsole ausgeführt (s. Abschnitt "Über Einschränkungen der Basisfunktionen" auf S. 70).

Funktion Systems Management

Es stehen folgende Funktionen zur Verfügung:

- Remote-Installation der Betriebssysteme
- Remote-Installation von Software-Updates, Suchen und Beheben von Schwachstellen
- Hardware-Inventarisierung
- lizenzierte Programmgruppen verwalten

- Remote-Verbindung mit Client-Geräten mithilfe der Microsoft® Windows®-Komponente Remotedesktopverbindung
- Remote-Verbindung mit Client-Geräten über Windows Desktopfreigabe
- Benutzerrollen verwalten.

Die Administrationseinheit für die Funktion Systems Management ist ein Client-Gerät in der Gruppe "Verwaltete Geräte".

> Im Funktionsumfang von Systems Management sind bei der Inventarisierung detaillierte Informationen über die Hardware der Geräte verfügbar.

> Damit Systems Management fehlerfrei funktioniert, müssen auf dem Laufwerk mindestens 100 GB freier Speicherplatz auf der Festplatte verfügbar sein.

Funktion Mobile Geräte verwalten

Die Funktion Mobile Geräte verwalten dient zur Verwaltung von Exchange ActiveSync- und mobilen iOS MDM-Geräten.

Für Exchange ActiveSync-Mobilgeräte sind folgende Funktionen verfügbar:

- Profile zur Verwaltung von mobilen Geräten erstellen und bearbeiten, den E-Mail-Postfächern der Benutzer Profile zuweisen
- Einstellungen für ein mobiles Gerät anpassen (E-Mail synchronisieren, Apps verwenden, Benutzerkennwort, Daten verschlüsseln, Wechselmedien anschließen)
- Zertifikate auf mobilen Geräten installieren.

Für mobile iOS MDM-Geräte sind folgende Funktionen verfügbar:

- Konfigurationsprofile erstellen und bearbeiten, Konfigurationsprofile auf mobilen Geräten installieren
- Anwendungen auf einem Mobilgerät über einen App Store® oder mithilfe von Property List-Dateien (.plist) installieren
- ein mobiles Gerät blockieren, Kennwort für ein mobiles Gerät zurücksetzen und alle Daten vom mobilen Gerät entfernen.

Außerdem ist im Rahmen der Funktion Mobile Geräte verwalten die Ausführung von Befehlen verfügbar, die für betreffende Protokolle vorgesehen sind.

Administrationseinheit für die Funktion Mobile Geräte verwalten ist das einzelne mobile Gerät. Ein mobiles Gerät gilt als verwaltet, sobald es zum Server für mobile Geräte verbunden wird.

Über Einschränkungen der Basisfunktionen

Vor der Aktivierung des Programms oder beim Ablauf der kommerziellen Lizenz wird Kaspersky Security Center im Modus Basisfunktionen der Administrationskonsole ausgeführt. Im Weiteren ist eine Beschreibung der Einschränkungen aufgeführt, die für die Funktion des Programms in diesem Modus gelten.

Mobile Geräte verwalten

Ein neues Profil kann nicht erstellt und einem mobilen Gerät (iOS MDM) bzw. Postfach (Exchange ActiveSync) zugewiesen werden. Die vorhandenen Profile können immer geändert und den Postfächern zugewiesen werden.

Programmverwaltung

Die Aufgaben zur Installation und zum Löschen von Updates können nicht gestartet werden. Alle Aufgaben, die vor dem Ablauf der Lizenz gestartet wurden, werden bis zum Ende ausgeführt; die letzten Updates werden aber nicht installiert. Wenn beispielsweise eine Aufgabe zur Installation von kritischen Updates vor dem Ablauf der Lizenz gestartet wurde, werden nur die kritischen Updates installiert, die vor dem Ablauf der Lizenz gefunden wurden.

Der Start und die Bearbeitung von Synchronisierungsaufgaben, die Suche nach Schwachstellen und das Update der Datenbank für Schwachstellen sind jederzeit verfügbar. Die Anzeige, Suche und Sortierung von Einträgen in der Liste der Schwachstellen und Updates unterliegen auch keinen Einschränkungen.

Remote-Installation von Betriebssystemen und Programmen

Die Aufgaben zum Erstellen und zur Installation des Betriebssystem-Abbilds können nicht gestartet werden. Die Aufgaben, die vor dem Ablauf der Lizenz gestartet wurden, werden bis zum Ende ausgeführt.

Hardware-Inventarisierung

Der Empfang von Informationen über neue Geräte mithilfe des Servers für mobile Geräte ist nicht verfügbar. Dabei werden Informationen über Computer und angeschlossene Geräte aktualisiert.

Die Benachrichtigungen über eine Änderung der Gerätekonfiguration funktionieren nicht.

Die Liste der Hardware kann nicht angezeigt und manuell bearbeitet werden.

Lizenzierte Programmgruppen verwalten

Ein neuer Schlüssel kann nicht hinzugefügt werden.

Es werden keine Benachrichtigungen darüber versandt, dass die Einschränkungen für die Nutzung der Schlüssel überschritten wurden.

Remote-Verbindung mit den Client-Geräten

Eine Remote-Verbindung mit den Client-Geräten ist nicht verfügbar.

Antiviren-Sicherheit

Ein Antiviren-Programm verwendet die Datenbanken, die vor dem Ablauf der Gültigkeitsdauer der Lizenz installiert wurden.

Über den Aktivierungscode

Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus zwanzig Buchstaben und Ziffern. Den Aktivierungscode geben Sie ein, um einen Schlüssel zur Aktivierung von Kaspersky Security Center hinzuzufügen. Sie erhalten den Aktivierungscode an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie Kaspersky Security Center erworben haben oder eine Testversion von Kaspersky Security Center bestellt haben.

Zur Aktivierung des Programms mithilfe eines Aktivierungscodes ist ein Internetzugang erforderlich, um sich mit den Aktivierungsservern von Kaspersky Lab zu verbinden.

Wenn das Programm mithilfe eines Aktivierungscodes aktiviert wurde, sendet das Programm in einigen Fällen nach der Aktivierung regelmäßige Anfragen an die Aktivierungsserver von Kaspersky Lab zur Überprüfung des aktuellen Schlüsselstatus. Zum Versenden von Anfragen benötigt das Programm Internetzugang.

Wenn der Aktivierungscode nach der Aktivierung des Programms verloren geht, können Sie ihn wiederherstellen. Der Aktivierungscode kann beispielsweise für die Registrierung im Kaspersky CompanyAccount erforderlich sein. Wenden Sie sich an den Technischen Support von Kaspersky Lab, um den Aktivierungscode wiederherzustellen (s. Abschnitt "Über den Technischen Support" auf S. 375).

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky Lab erhalten. Die Schlüsseldatei dient dazu, einen Schlüssel für die Aktivierung des Programms hinzuzufügen.

Sie erhalten die Schlüsseldatei an die von Ihnen angegebene E-Mail-Adresse, nachdem Sie Kaspersky Security Center erworben oder eine Testversion von Kaspersky Security Center bestellt haben.

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

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

Zur Wiederherstellung der Schlüsseldatei müssen Sie eine der folgenden Aktionen ausführen:

- Wenden sich an Technischen Support (http://support.kaspersky.com/de).
- Schlüsseldatei anhand eines vorhandenen Aktivierungscodes auf der Website von Kaspersky Lab (https://activation.kaspersky.com/de/) abrufen.

Über das Abonnement

Ein *Abonnement für Kaspersky Security Center* ist eine Bestellung des Programms mit bestimmten Einstellungen (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Security Center kann bei einem Lieferanten von Dienstleistungen abgeschlossen werden (z. B. bei einem Internet-Provider). Das Abonnement kann manuell oder automatisch verlängert oder auch gekündigt werden.

Ein Abonnement kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt sein (ohne Ablaufdatum). Um Kaspersky Security Center weiterhin zu nutzen, muss ein beschränktes Abonnement rechtzeitig verlängert werden. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstleister überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abonnement-Verlängerung gewährt, während der die Funktionalität der Anwendung erhalten bleibt. Verfügbarkeit und Dauer der Nachfrist werden vom Lieferanten der Dienstleistungen bestimmt.

Um Kaspersky Security Center mit einem Abonnement zu nutzen, muss der Aktivierungscode übernommen werden, den Sie von Ihrem Provider erhalten.

Sie können nur dann einen anderen Aktivierungscode für die Nutzung von Kaspersky Security Center verwenden, wenn das Abonnement zuvor abgelaufen ist oder gekündigt wurde.

Für die Abonnement-Verwaltung stehen je nach Provider unterschiedliche Optionen zur Verfügung. Der Provider stellt möglicherweise keine Nachfrist für die Verlängerung des Abonnements zur Verfügung, innerhalb der die Funktionen der Anwendung erhalten bleiben.

Die für ein Abonnement erhaltenen Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Security Center verwendet werden.

Bei einer Nutzung des Programms im Abonnement stellt Kaspersky Security Center zum festgelegten Zeitpunkt vor Ablauf des Abonnements automatisch eine Verbindung zum Aktivierungsserver her. Sie können das Abonnement auf der Website des Providers verlängern.

Schnellstartassistent für den Administrationsserver

Dieser Abschnitt enthält Informationen zum Schnellstartassistenten für den Administrationsserver.

Kaspersky Security Center bietet die Möglichkeit, mithilfe des Schnellstartassistenten eine minimale Auswahl von Einstellungen zu konfigurieren, die für die Einrichtung des Systems zur zentralen Verwaltung des Antiviren-Schutzes benötigt werden. Während der Ausführung des Assistenten werden im Programm folgende Änderungen vorgenommen:

- Es werden Schlüssel oder Codes hinzugefügt, die automatisch auf die Geräte der Administrationsgruppen verteilt werden können.
- Die Interaktion mit Kaspersky Security Network (KSN) wird eingerichtet. KSN ermöglicht den Abruf von Informationen über die auf den verwalteten Geräten installierten Programme aus den Kaspersky Lab-Reputations-Datenbanken. Wenn Sie die Verwendung von KSN zugelassen haben, aktiviert der Assistent den Dienst des KSN-Proxyservers, mit dem die Interaktion zwischen KSN und den Geräten gewährleistet wird.
- Es wird ein E-Mail-Versand von Benachrichtigungen über Ereignisse konfiguriert, die vom Administrationsserver und den verwalteten Programmen registriert werden. Damit Benachrichtigungen erfolgreich zugestellt werden, muss auf dem Administrationsserver und allen Geräten der Windows Messenger Dienst gestartet werden.
- Die Einstellungen für das Update und das Schließen von Schwachstellen der auf den Geräten installierten Programme werden angepasst.
- Für die oberste Hierarchieebene der verwalteten Geräte werden Schutzrichtlinien für Arbeitsstationen und Server sowie Aufgaben Virensuche, Update-Download und Verschieben ins Backup erstellt.

Der Schnellstartassistent erstellt Schutzrichtlinien nur für Programme, für die es noch keine Richtlinien im Ordner **Verwaltete Geräte** gibt. Der Schnellstartassistent erstellt keine Aufgaben, deren Namen mit den Aufgabennamen übereinstimmen, die für die obere Hierarchieebene der verwalteten Geräte bereits erstellt wurden.

Das Programm schlägt vor, beim ersten Verbindungsaufbau zum Server nach der Installation des Administrationsservers den Schnellstartassistenten zu starten. Der Schnellstartassistent kann auch manuell aus dem Kontextmenü des Knotens **Administrationsserver <Gerätename>** gestartet werden.

Grundbegriffe

Dieser Abschnitt enthält ausführliche Definitionen der Grundbegriffe zu Kaspersky Security Center.

In diesem Abschnitt

Administrationsserver

Die Komponenten von Kaspersky Security Center ermöglichen eine Remote-Programmverwaltung der auf Client-Geräten installierten Kaspersky-Lab-Programme.

Geräte, auf welchen die Komponente Administrationsserver installiert ist, werden als *Administrationsserver* bezeichnet (im Weiteren auch *Server* genannt).

Der Administrationsserver wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Unter dem Namen "Kaspersky Security Center Administrationsserver"
- mit automatischem Start bei Start des Betriebssystems
- Unter dem Benutzerkonto **Lokales System** oder unter dem Benutzerkonto, das bei Installation des Administrationsservers ausgewählt wurde.

Der Administrationsserver führt folgende Funktionen aus:

- Speicherung der Struktur der Administrationsgruppen
- Speicherung von Informationen über die Konfiguration der Client-Geräte
- Organisation der Speicherordner für Programmdateien
- Remote-Installation von Programmen auf Client-Geräten und Löschen von Programmen
- Datenbanken-Update und Update der Programm-Module von Kaspersky Lab
- Verwaltung von Richtlinien und Aufgaben auf Client-Geräten
- Speicherung von Informationen über die auf den Client-Geräten aufgetretenen Ereignisse
- Erstellen von Berichten über die Ausführung von Kaspersky-Lab-Programmen
- Verteilung von Schlüsseln auf Client-Geräte, Speicherung von Schlüsseldaten
- Senden von Benachrichtigungen über den Status der Aufgabenausführung (z. B. über einen Virenfund auf einem Client-Gerät).

Hierarchie der Administrationsserver

Die Administrationsserver können eine Hierarchie der Art "Hauptserver – untergeordneter Server" bilden. Jeder Administrationsserver kann über mehrere untergeordnete Administrationsserver (im Folgenden auch *untergeordnete Server*) auf verschiedenen Hierarchieebenen verfügen. Die Verschachtelungstiefe der untergeordneten Server ist nicht beschränkt. Zu den Administrationsgruppen des Hauptservers gehören die Client-Geräte aller untergeordneten Server. So können unabhängige Bereiche des Computernetzwerks durch

verschiedene Administrationsserver verwaltet werden, die wiederum durch einen Hauptserver administriert werden.

Ein *virtueller Administrationsserver* stellt einen besonderen Fall eines untergeordneten Administrationsservers dar (s. Abschnitt "Virtueller Administrationsserver" auf S. 80).

Die Hierarchie der Administrationsserver lässt sich zu folgenden Zwecken verwenden:

- Beschränkung der Belastung des Administrationsservers (im Vergleich zu einem einzigen im Netzwerk installierten Server).
- Verringerung des Datenverkehrs im Netzwerk und Vereinfachung der Arbeit mit Remote-Niederlassungen. Es muss keine Verbindung zwischen dem Hauptserver und allen Geräten im Netzwerk bestehen, die sich zum Beispiel in anderen Regionen befinden. Es genügt, wenn in jedem Segment des Netzwerks ein untergeordneter Administrationsserver installiert ist, die Geräte auf Administrationsgruppen der untergeordneten Server verteilt werden und für die untergeordneten Server eine schnelle Verbindung zum Hauptserver besteht.
- Verteilung der Verantwortung zwischen den Administratoren für den Antiviren-Schutz. Dabei bleiben alle Möglichkeiten der zentralen Verwaltung und der Überwachung des Status des Antiviren-Schutzes im Unternehmensnetzwerk erhalten.
- Nutzung von Kaspersky Security Center von Dienstanbietern. Ein Dienstanbieter kann Kaspersky Security Center und die Kaspersky Security Center 10 Web Console installieren. Um eine große Anzahl an Client-Geräten verschiedener Unternehmen zu verwalten, kann der Dienstanbieter virtuelle Administrationsserver zur Hierarchie der Administrationsserver hinzufügen.

Jedes Gerät, das zur Hierarchie der Administrationsgruppen gehört, kann nur mit einem Administrationsserver verbunden sein. Sie müssen die Verbindung der Geräte mit den Administrationsservern selbständig prüfen. Dazu können Sie die Suche-Funktion der Geräte nach Netzwerkattributen in den Administrationsgruppen verschiedener Server verwenden.

Virtueller Administrationsserver

Ein virtueller Administrationsserver (im Folgenden auch *Virtueller Server* genannt) ist eine Komponente des Programms Kaspersky Security Center, die dazu konzipiert ist, das Netzwerk eines Kundenunternehmens zu verwalten.

Ein virtueller Administrationsserver stellt einen besonderen Fall eines untergeordneten Administrationsservers dar und weist im Vergleich zu einem physikalischen Administrationsserver folgende Einschränkungen auf:

- Ein virtueller Administrationsserver kann nur dann funktionieren, wenn er zum Hauptadministrationsserver gehört.
- Ein virtueller Administrationsserver verwendet die Datenbank des Hauptadministrationsservers: Aufgaben zum Erstellen von Sicherungskopien und zur Datenwiederherstellung, Aufgaben zur Update-Überprüfung und Aufgaben zum Download von Updates werden auf dem virtuellen Server nicht unterstützt. Diese Aufgaben werden auf dem Hauptadministrationsserver ausgeführt.
- Für virtuelle Server können keine untergeordneten Administrationsserver angelegt werden (einschl. virtueller Server).

Außerdem weisen virtuelle Administrationsserver folgende Einschränkungen auf:

- Es gibt weniger Abschnitte im Eigenschaftenfenster des virtuellen Servers.
- Um eine Remote-Installation von Kaspersky Lab-Programmen auf Geräten vorzunehmen, die vom virtuellen Server verwaltet werden, muss auf einem der Geräte der Administrationsagent installiert sein, über den eine Verbindung zum virtuellen Server aufgebaut werden kann. Beim ersten Verbindungsaufbau zum virtuellen Server wird diesem Gerät automatisch die Rolle des Update-Agenten zugewiesen, sodass er als Verbindungs-Gateway für den Anschluss von Client-Geräten an den virtuellen Server dient.

- Der virtuelle Server kann das Netzwerk nur durch die Update-Agenten durchsuchen.
- Um einen virtuellen Server neu zu starten, der in seiner Funktionsfähigkeit beeinträchtigt wurde, startet Kaspersky Security Center den Hauptadministrationsserver und alle virtuellen Server neu.

Der Administrator eines virtuellen Servers verfügt über alle Rechte für diesen virtuellen Server.

Server für mobile Geräte

Beim *Server für mobile Geräte* handelt es sich um eine Komponente von Kaspersky Security Center, die Zugriff auf mobile Geräte und deren Verwaltung über die Verwaltungskonsole ermöglicht. Der Server für mobile Geräte empfängt Informationen über mobile Geräte und speichert ihre Profile.

Es sind zwei Arten von Servern für mobile Geräte vorhanden:

- Exchange ActiveSync-Server für mobile Geräte Dieser Server wird auf dem Gerät installiert, auf dem ein Microsoft Exchange-Server installiert wurde, und ermöglicht es, Daten vom Microsoft Exchange-Server abzurufen und sie auf den Administrationsserver zu übertragen. Mit diesem Server für mobile Geräte können Sie mobile Geräte verwalten, die das Exchange ActiveSync-Protokoll unterstützen.
- iOS MDM-Server Mit diesem Server für mobile Geräte können Sie mobile Geräte verwalten, die den Dienst Apple Push Notification (APNs) unterstützen.

Die Server für mobile Geräte von Kaspersky Security Center ermöglichen die Verwaltung folgender Objekte:

- Ein einzelnes mobiles Gerät
- Mehrere mobile Geräte
- Mehrere mobile Geräte, die mit einem Server-Cluster verbunden sind (können gleichzeitig verwaltet werden). Bei der Verbindung mit einem Server-Cluster wird der in diesem Cluster installierte Server für mobile Geräte als ein einzelner Server in der Verwaltungskonsole angezeigt.

Webserver

Beim Kaspersky Security Center *Webserver* (im Folgenden auch *Webserver* genannt) handelt es sich um eine Kaspersky Security Center Komponente, 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.

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 autonomen Paketes abbrechen oder es erneut auf dem Webserver veröffentlichen.

Beim Erstellen eines iOS MDM-Profils für das mobile Gerät eines Benutzers wird das Profil automatisch auf dem Webserver veröffentlicht. Das veröffentlichte Profil wird automatisch vom Webserver entfernt, nachdem es auf dem mobilen Gerät des Benutzers erfolgreich installiert wurde (für weitere Details zum Erstellen und zur Installation des iOS MDM-Profils siehe: *Kaspersky Security Center Implementierungshandbuch*).

Der freigegebene Ordner wird zum Speichern von Informationen verwendet, die für alle Benutzer verfügbar sind, deren Geräte über den Administrationsserver verwaltet werden. Hat ein Benutzer keinen direkten Zugriff auf den freigegebenen Ordner, können die Informationen aus diesem Ordner mithilfe des Webservers an ihn übermittelt werden.

Um Informationen aus dem freigegebenen Ordner mithilfe des Webservers an Benutzer übermitteln zu können, soll der Administrator im Ordner einen Unterordner mit dem Namen public erstellen und die Informationen in diesen Unterordner kopieren.

Der Link für die Übermittlung der Informationen an den Benutzer soll folgendes Aussehen aufweisen:

```
https://<Webservername>:<HTTPS-Port>/public/<Objekt>,
```

wobei

- `<Webservername>` für den Namen des Kaspersky Security Center Webservers und
- `<HTTPS-Port>` für den vom Administrator angegebenen HTTP-Port des Webservers steht. Den HTTPS-Port können Sie im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers festlegen. Standardmäßig wird Port 8061 verwendet.
- Beim `<Objekt>` handelt es sich um einen Unterordner bzw. eine Datei, die für den Benutzer freigegeben werden sollen.

Der Administrator kann den erstellten Link auf jede Weise an den Benutzer übermitteln, wie etwa per E-Mail.

Mit diesem Link kann der Benutzer die für ihn vorgesehenen Informationen auf das lokale Gerät herunterladen.

Administrationsagent. Administrationsgruppe

Die Interaktion zwischen dem Administrationsserver und den Geräten gewährleistet die Programmkomponente von Kaspersky Security Center *Administrationsagent*.
Der Administrationsagent muss auf allen Geräten installiert werden, auf welchen Kaspersky Lab-Programme mit Kaspersky Security Center verwaltet werden.

Der Administrationsagent wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Unter dem Namen "Kaspersky Security Center Administrationsagent"
- mit automatischem Start bei Start des Betriebssystems
- mit dem Benutzerkonto **Lokales System**.

Ein Gerät, ein Server oder eine Workstation, auf der der Administrationsagent und verwaltete Programme von Kaspersky Lab installiert sind, wird als *Administrationsserver-Client* bezeichnet (im Folgenden *Client-Gerät* oder *Gerät* genannt).

Die zahlreichen Geräte in einem Unternehmensnetzwerk lassen sich in Gruppen aufteilen, die eine hierarchische Struktur bilden. Solche Gruppen werden als *Administrationsgruppen* bezeichnet. Die Hierarchie der Administrationsgruppen wird in der Konsolenstruktur im Knoten des Administrationsservers dargestellt.

Bei einer *Administrationsgruppe* (im Folgenden *Gruppe* genannt) handelt es sich um eine Gruppe von Client-Geräten, die nach einem beliebigen Merkmal zusammengefasst sind und als geschlossene Einheit verwaltet werden können. Auf jedem Client-Gerät in einer Gruppe gelten:

- einheitliche Einstellungen für Anwendungen mithilfe von *Gruppenrichtlinien*
- einheitlicher Modus für Programme durch Erstellen von *Gruppenaufgaben* mit bestimmten Einstellungen (z. B. Erstellung und Installation eines einheitlichen *Installationspakets*, Update der Datenbanken und Programm-Module, Untersuchung des Geräts auf Befehl und Echtzeitschutz).

Ein Client-Gerät kann nur zu einer Administrationsgruppe gehören.

Sie können eine Hierarchie der Server und Gruppen mit beliebiger Verschachtelungstiefe erstellen. Auf einer Hierarchieebene können sich untergeordnete und virtuelle Administrationsserver, Gruppen und Client-Geräte befinden.

Administrator-Arbeitsplatz

Geräte, auf welchen die Komponente *Verwaltungskonsole* installiert ist, werden als *Administrator-Arbeitsplätze* bezeichnet. Von diesen Geräten aus können die Administratoren eine zentralisierte Remote-Programmverwaltung für die auf den Client-Geräten installierten Kaspersky Lab-Programme durchführen.

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

Die Anzahl an Administrator-Arbeitsplätzen ist nicht beschränkt. Von jedem Administrator-Arbeitsplatz aus können Administrationsgruppen mehrerer Administrationsserver zugleich verwaltet werden. Der Administrator-Arbeitsplatz kann mit dem Administrationsserver (physischen oder virtuellen) einer beliebigen Hierarchieebene verbunden werden.

Der Administrator-Arbeitsplatz kann in eine Administrationsgruppe als Client-Gerät aufgenommen werden.

Im Rahmen von Administrationsgruppen eines beliebigen Servers kann dasselbe Gerät sowohl Client des Administrationsservers als auch Administrationsserver und Administrator-Arbeitsplatz sein.

Verwaltungs-Plug-in für das Programm

Die Verwaltung von Kaspersky-Lab- Programmen über die Administrationskonsole erfolgt mit einer speziellen Komponente, nämlich *Verwaltungs-Plug-in für das Programm*. Die Komponente gehört zu allen Kaspersky-Lab-Anwendungen, deren Verwaltung mit Kaspersky Security Center möglich ist.

Das Verwaltungs-Plug-in für das Programm wird auf dem Administrator-Arbeitsplatz installiert. Mithilfe des Verwaltungs-Plug-ins für das Programm können Sie über die Verwaltungskonsole folgende Aktionen ausführen:

- Richtlinien erstellen sowie Programmeinstellungen und Aufgabeneinstellungen des Programms bearbeiten
- Informationen über Programmaufgaben und Ereignisse, die während der Programmausführung auftreten, sowie Statistiken zur Programmausführung von Client-Geräten abrufen.

Richtlinien, Programmeinstellungen und Aufgaben

Eine festgelegte Aktion, die von einem Kaspersky-Lab-Programm ausgeführt wird, wird als *Aufgabe* bezeichnet. Je nach den auszuführenden Funktionen werden Aufgaben nach *Typen* unterschieden.

Jede Aufgabe entspricht einer Kombination von Anwendungseinstellungen, die bei ihrer Ausführung zur Anwendung kommen. Bei dem Anwendungseinstellungssatz, der für alle Aufgabentypen gleich ist, handelt es sich um die Anwendungseinstellungen.
Die Anwendungseinstellungen, die für jeden Aufgabentyp separat gelten, bilden die Aufgabeneinstellungen.

> Eine detaillierte Beschreibung der Aufgabentypen für jedes Kaspersky-Lab-Programm finden Sie in den jeweiligen Handbüchern.

Die Programmeinstellungen, die für jedes einzelne Client-Gerät über die lokale Programmoberfläche oder im Remote-Modus über die Verwaltungskonsole definiert werden, werden als *lokale Einstellungen der Anwendung* bezeichnet.

Die zentrale Konfiguration der Einstellungen für die Programme, die auf den Client-Geräten installiert sind, erfolgt über Richtlinien.

Bei einer *Richtlinie* handelt es sich um eine Gruppe von Programmeinstellungen, die für eine Administrationsgruppe definiert wurden. Nicht alle Anwendungseinstellungen werden durch eine Richtlinie definiert.

Für eine Anwendung können mehrere Richtlinien mit verschiedenen Einstellungswerten definiert werden, es kann jedoch nur eine Richtlinie für die Anwendung aktiv sein.

Das Einstellen einer Anwendung kann für verschiedene Gruppen unterschiedlich sein. In jeder Gruppe kann eine eigene Richtlinie für ein Programm angelegt werden.

Die Anwendungseinstellungen werden durch Richtlinieneinstellungen und Aufgabeneinstellungen definiert.

Untergruppen und untergeordnete Administrationsserver erhalten die Aufgaben der Gruppen der höheren Hierarchieebenen durch Vererbung. Eine Gruppenaufgabe wird nicht nur auf den Client-Geräten der entsprechenden Gruppe ausgeführt, sondern auch auf den Client-Geräten der Untergruppen und untergeordneten Server auf allen nachfolgenden Hierarchieebenen.

Jede Einstellung der Richtlinie weist das Attribut "Schloss" auf:  . Das "Schloss" zeigt, ob eine Änderung der Einstellung in den Richtlinien der untergeordneten Hierarchieebene (für Untergruppen und untergeordnete Administrationsserver), in den Aufgabeneinstellungen und in den lokalen Programmeinstellungen verboten ist. Wenn in der Richtlinie für die Einstellung ein "Schloss" gesetzt ist, lässt sich der Wert nicht verändern (s. Abschnitt "Interaktion von Richtlinie und lokalen Programmeinstellungen" auf S. 88).

Wenn Sie im Eigenschaftenfenster der geerbten Richtlinie das Kontrollkästchen **Einstellungen aus Richtlinie der höheren Ebene erben** deaktivieren, das sich unter **Einstellungen erben** im Abschnitt **Allgemein** befindet, wird die Wirkung des "Schlosses" für diese Richtlinie aufgehoben.

Es ist eine Option vorgesehen, die eine inaktive Richtlinie bei Eintritt eines Ereignisses aktiviert. Dadurch können beispielsweise strengere Einstellungen des Antiviren-Schutzes bei Virenepidemien festgelegt werden.

Außerdem lässt sich eine mobile Richtlinie erstellen.

Aufgaben für Objekte, die von einem Administrationsserver verwaltet werden, werden zentral angelegt und konfiguriert. Es lassen sich folgende Aufgabentypen definieren:

- *Gruppenaufgabe* – Aufgabe, welche die Einstellungen der Programme definiert, die auf den Geräten der Administrationsgruppe installiert sind
- *Lokale Aufgabe* – Aufgabe für ein einzelnes Gerät
- *Aufgabe für bestimmte Geräte* – Aufgabe für eine beliebige Auswahl an Geräten, unabhängig davon, ob sie zu einer Administrationsgruppe gehören
- *Aufgabe des Administrationsservers* – Aufgabe, die unmittelbar für den Administrationsserver definiert wird.

In einer Gruppe kann eine Gruppenaufgabe sogar dann definiert werden, wenn das Kaspersky Lab-Programm nicht auf allen Client-Geräten der Gruppe installiert wurde.

In diesem Fall wird die Gruppenaufgabe nur für die Geräte ausgeführt, auf welchen das angegebene Programm installiert ist.

> Aufgaben, die für ein Client-Gerät lokal erstellt wurden, werden nur für dieses Gerät ausgeführt. Bei der Synchronisierung des Client-Geräts mit dem Administrationsserver werden die lokalen Aufgaben zur Liste der Aufgaben hinzugefügt, die für das Client-Gerät erstellt wurden.

Da die Anwendungseinstellungen durch eine Richtlinie definiert werden, können in den Aufgabeneinstellungen diejenigen Einstellungen neu bestimmt werden, deren Änderung in der Richtlinie nicht unterbunden ist, sowie diejenigen Einstellungen, die nur für das konkrete Exemplar der Aufgabe gesetzt werden können. Dies gilt zum Beispiel bei einer Aufgabe zur Untersuchung eines Datenträgers für den Namen des Datenträgers und der Maske der zu untersuchenden Dateien.

Aufgaben können automatisch (nach Zeitplan) oder manuell gestartet werden. Die Ergebnisse der Aufgabenausführung werden auf dem Administrationsserver und lokal gespeichert. Der Administrator kann sich benachrichtigen lassen, wie die jeweilige Aufgabe ausgeführt wurde, und detaillierte Berichte einsehen.

Daten zu Richtlinien, Anwendungseinstellungen, Einstellungen für die Aufgaben für bestimmte Geräte und Gruppenaufgaben werden auf dem Server gespeichert und bei der Synchronisierung auf die Client-Geräte verteilt. Dabei werden Daten über lokale Änderungen, die von der Richtlinie zugelassen und auf den Client-Geräten vorgenommen werden, auf dem Administrationsserver gespeichert. Außerdem werden die Liste der auf dem Client-Gerät laufenden Programme sowie deren Status und die Liste der angelegten Aufgaben aktualisiert.

Interaktion von Richtlinie und lokalen Programmeinstellungen

Mit Richtlinien können identische Funktionseinstellungen einer Anwendung für alle Geräte gesetzt werden, die zu einer Gruppe gehören.

Die Einstellungswerte, die durch eine Richtlinie vorgegeben werden, lassen sich für einzelne Geräte mit lokalen Anwendungseinstellungen ändern. Dabei können die Werte nur

für die Einstellungen festgelegt werden, deren Änderung nicht durch die Richtlinie unterbunden ist, wenn die Einstellung also kein verriegeltes Schloss aufweist.

Den Wert, den das Programm auf dem Client-Gerät verwendet (s. Abb. unten), wird durch das Schloss an der Einstellung in der Richtlinie definiert:

- Wenn die Änderung der Einstellung unterbunden ist, wird auf allen Client-Geräten der gleiche Wert verwendet, der von der Richtlinie vorgegeben ist.
- Wenn die Änderung nicht unterbunden ist, verwendet das Programm den lokalen Einstellungswert auf jedem Client-Gerät und nicht den Wert, der in der Richtlinie angegeben ist. Der Einstellungswert kann dabei über die lokalen Anwendungseinstellungen geändert werden.

Abbildung 7. Richtlinie und lokale Programmeinstellungen

So verwendet das Programm bei Ausführung der Aufgabe auf dem Client-Gerät die Einstellungen, welche auf zwei verschiedene Arten vorgegeben sind:

- durch die Aufgabeneinstellungen und die lokalen Anwendungseinstellungen, wenn in der Richtlinie die Änderung der Einstellung nicht unterbunden wurde
- durch die Richtlinie der Gruppe, wenn in der Richtlinie die Änderung der Einstellung unterbunden wurde.

Die lokalen Anwendungseinstellungen werden nach der ersten Anwendung der Richtlinie mit den Richtlinieneinstellungen überschrieben.

Update-Agent

Der Update-Agent ist ein Gerät mit installiertem Administrationsagenten, der für die Verteilung von Updates, die Remote-Installation von Programmen und den Empfang von Informationen über Geräte im Netzwerk verwendet wird. Der Update-Agent kann folgende Funktionen ausüben:

- Updates und Installationspakete, die vom Administrationsserver heruntergeladen wurden, auf die Client-Geräte der Gruppe verteilen (einschließlich mittels Broadcast über das UDP-Protokoll). Updates können sowohl vom Administrationsserver als auch von den Kaspersky-Lab-Update-Servern empfangen werden. Im letzteren Fall muss für das Gerät, das als Update-Agent fungiert, eine Update-Aufgabe erstellt werden (s. Abschnitt "Updates für Kaspersky Endpoint Security auf Client-Geräten automatisch installieren" auf S. 242).

  Update-Agenten beschleunigen die Update-Verteilung und ermöglichen, die Belastung des Administrationsservers zu verringern.

- Richtlinien und Gruppenaufgaben mit dem Broadcast über das UDP-Protokoll verteilen.

- Die Rolle eine Verbindungs-Gateways zum Administrationsserver für die Geräte der Administrationsgruppe ausführen (s. Abschnitt "Update-Agenten als Gateway verwenden" auf S. 414).

  Wenn keine Möglichkeit besteht, eine direkte Verbindung zwischen den verwalteten Geräten und dem Administrationsserver herzustellen, können Sie den Update-Agenten zum Gateway für Verbindungen dieser Gruppe mit dem Administrationsserver bestimmen.

In diesem Fall werden die verwalteten Geräte mit dem Verbindungs-Gateway verbunden, das seinerseits mit dem Administrationsserver verbunden wird.

Das Vorhandensein eines Update-Agenten, der die Rolle des Verbindungs-Gateways übernimmt, schließt eine direkte Verbindung der verwalteten Geräte mit dem Administrationsserver nicht aus. Wenn das Verbindungs-Gateway nicht verfügbar ist, aber eine direkte Verbindung mit dem Administrationsserver möglich ist, werden die verwalteten Geräte direkt mit dem Server verbunden.

- Netzwerk mit dem Ziel abfragen, neue Geräte und aktualisierte Informationen über die gefundenen Geräte zu finden. Der Update-Agent kann dieselben Arten von Netzwerkabfragen ausführen wie der Administrationsserver.

- Remote-Installation von Programmen sowohl von Drittanbietern als auch von Kaspersky Lab mit Microsoft Windows-Mitteln durchführen, unter anderem auch auf Client-Geräten ohne installiertem Administrationsagenten.

  Diese Funktion ermöglicht es, Installationspakete des Administrationsagenten auf Client-Geräte zu übertragen, die sich in Netzwerken befinden, auf die der Administrationsserver nicht direkt zugreifen kann.

Die Übertragung von Dateien vom Administrationsserver an den Update-Agenten wird über das HTTP-Protokoll oder das HTTPS-Protokoll (wenn die Verwendung von SSL-Verbindungen konfiguriert ist) umgesetzt. Die Verwendung des HTTP- oder HTTPS-Protokolls gewährleistet im Vergleich zum SOAP-Protokoll aufgrund des reduzierten Datenverkehrs eine höhere Leistung.

Geräte mit installiertem Administrationsagenten können manuell vom Administrator oder automatisch durch den Administrationsserver als Update-Agent festgelegt werden (s. Abschnitt "Geräte zum Update-Agenten bestimmen" auf S. 346). Eine vollständige Liste der Update-Agenten für die angegebenen Administrationsgruppen können Sie sich anzeigen lassen, indem Sie einen Bericht zur Liste der Update-Agenten erstellen.

Der Gültigkeitsbereich des Update-Agenten ist eine Administrationsgruppe, für die der Update-Agent vom Administrator bestimmt wurde, sowie ihre Untergruppen auf jeder Verschachtelungstiefe. Wurden in der Hierarchie der Administrationsgruppen mehrere Update-Agenten bestimmt, wird der Administrationsagent des verwalteten Geräts mit dem Update-Agenten verbunden, der in der Hierarchie als nächster steht.

Als Gültigkeitsbereich des Update-Agenten kann auch ein NLA-Subnet fungieren. Das NLA-Subnet wird zum Erstellen einer manuellen Auswahl von Geräten verwendet, auf die der Update-Agent Updates verteilt.

Wenn die Update-Agenten automatisch vom Administrationsserver bestimmt werden, dann werden die Update-Agenten vom Server anhand der Broadcast-Domänen und nicht anhand der Administrationsgruppen bestimmt. Dies geschieht nachdem die Broadcast-Domäne bestimmt wurde. Der Administrationsagent führt einen Nachrichtenaustausch mit den anderen Administrationsagenten seines Subnetzes aus und sendet dem Administrationsserver Informationen über sich sowie Kurzinformationen über die anderen Administrationsagenten. Auf der Grundlage dieser Informationen kann der Administrationsserver eine Gruppierung der Administrationsagenten anhand der Broadcast-Domänen durchführen. Die Broadcast-Domänen werden dem Administrationsserver bekannt, nachdem mehr als 70 % der Administrationsagenten in den Administrationsgruppen durchsucht wurden. Der Administrationsserver durchsucht die Broadcast-Domänen alle zwei Stunden.

> Nachdem die Update-Agenten anhand der Broadcast-Domänen bestimmt wurden, können sie nicht mehr neu anhand von Administrationsgruppen bestimmt werden.

> Administrationsagenten mit aktivem Verbindungsprofil nehmen nicht an der Bestimmung der Broadcast-Domäne teil.

Wenn in einem Netzwerksegment oder einer Administrationsgruppe zwei oder mehr Update-Agenten bestimmt werden, wird einer davon aktiv, und die anderen bleiben in Reserve. Der aktive Update-Agent lädt Updates und Installationspakete unmittelbar vom Administrationsserver herunter, die Reserve-Update-Agenten fragen nur den aktiven Update-Agenten nach Updates ab. In diesem Fall werden Dateien nur einmal vom Administrationsserver heruntergeladen und im Weiteren auf die Update-Agenten verteilt. Sollte der aktive Update-Agent aus irgendwelchen Gründen offline sein, wird einer der Reserve-Update-Agenten zum aktiven bestimmt. Der Administrationsserver bestimmt die Reserve-Update-Agenten automatisch.

> Der Status des Update-Agenten (*Aktiv* / *Reserve*) wird durch ein Kontrollkästchen im Bericht des Tools klnagchk angezeigt (s. Abschnitt "Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk" auf S. 161).

Für die Ausführung des Update-Agenten sind mindestens 4 GB freier Speicherplatz auf der Festplatte erforderlich. Wenn der freie Speicherplatz auf dem Laufwerk des Update-Agenten weniger als 2 GB beträgt, erstellt Kaspersky Security Center einen Vorfall der Ereigniskategorie *Warnung*. Der Vorfall wird in den Eigenschaften des Geräts im Abschnitt **Vorfälle** veröffentlicht.

Wenn auf dem Administrationsserver Aufgaben zur Remote-Installation vorhanden sind, ist auf dem Gerät mit dem Update-Agenten zusätzlicher Speicherplatz in der Größe erforderlich, die der Summe aller zu installierenden Installationspakete entspricht.

Wenn auf dem Administrationsserver ein oder mehrere Exemplare einer Aufgabe zur Installation von Updates (Patches) und zum Schließen von Schwachstellen vorhanden sind, ist auf dem Gerät mit dem Update-Agenten zusätzlicher Speicherplatz in der Größe erforderlich, die der doppelten Summe aller zu installierenden Patches erforderlich.

Administrationsserver verwalten

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsservern und deren Einstellungen.

In diesem Abschnitt

Verbindung mit dem Administrationsserver herstellen und zwischen Administrationsservern wechseln

Beim Starten versucht Kaspersky Security Center, eine Verbindung zum Administrationsserver herzustellen. Wenn im Netzwerk mehrere Administrationsserver vorhanden sind, wird der Server abgefragt, mit dem eine Verbindung während der letzten Sitzung von Kaspersky Security Center hergestellt wurde.

Wenn das Programm zum ersten Mal nach der Installation gestartet wird, wird eine Verbindung mit dem Administrationsserver hergestellt, der bei der Installation von Kaspersky Security Center angegeben wurde.

Nachdem die Verbindung mit dem Administrationsserver hergestellt wurde, wird die Ordnerstruktur dieses Servers in der Konsolenstruktur angezeigt.

Wurden zur Konsolenstruktur mehrere Administrationsserver hinzugefügt, können Sie zwischen ihnen wechseln.

Um zu einem anderen Administrationsserver zu wechseln, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Mit dem Administrationsserver verbinden** aus.

3. Geben Sie im folgenden Fenster **Verbindungseinstellungen** im Feld **Serveradresse** den Namen des Administrationsservers an, mit dem eine Verbindung hergestellt werden soll. Als Name des Administrationsservers können Sie die IP-Adresse oder den Gerätenamen im Windows-Netzwerk angeben. Mit der Schaltfläche **Erweitert** im unteren Bereich des Fensters können Sie die Verbindungseinstellungen mit dem Administrationsserver anpassen.

Zur Verbindung mit dem Administrationsserver über einen Port, der sich vom standardmäßigen Port unterscheidet, geben Sie im Feld **Serveradresse** einen Wert im Format <Name des Administrationsservers>:<Port> an.

Die Benutzer, die über keine Berechtigung zum **Lesen** verfügen, können nicht auf den Administrationsserver zugreifen.

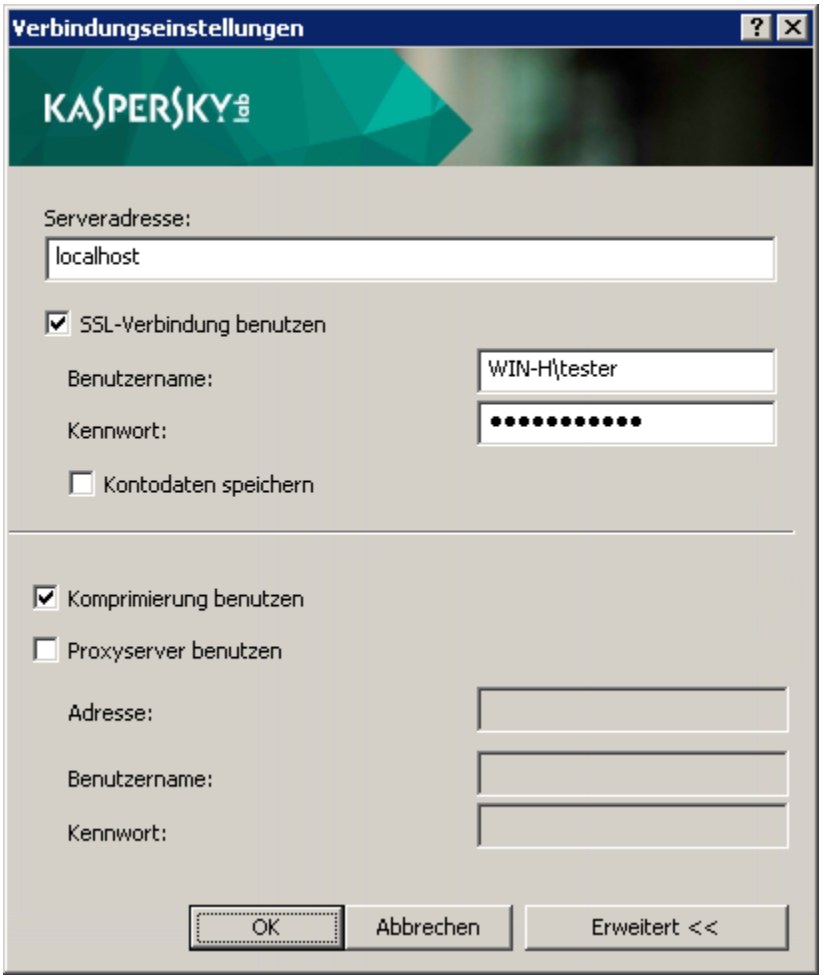


Abbildung 8. Verbindung zum Administrationsserver herstellen

4. Klicken Sie auf **OK**, um das Umschalten zwischen den Servern abzuschließen.

Nach der Verbindung mit dem Administrationsserver wird die Ordnerstruktur des entsprechenden Knotens in der Konsolenstruktur aktualisiert.

Zugriffsberechtigungen für den Administrationsserver und dessen Objekte

Bei der Installation von Kaspersky Security Center werden die Benutzergruppen **KLAdmins** und **KLOperators** automatisch erstellt. Diesen Gruppen werden die Rechte für die Verbindung mit dem Administrationsserver und die Bearbeitung der Serverobjekte gewährt.

Abhängig davon, unter welchem Benutzerkonto Kaspersky Security Center installiert wird, werden die Gruppen **KLAdmins** und **KLOperators** auf folgende Weise erstellt:

- Wenn die Installation unter dem Benutzerkonto eines Benutzers ausgeführt wird, der zur Domäne gehört, werden die Gruppen in der Domäne, zu der der Administrationsserver gehört, sowie auf dem Administrationsserver erstellt.
- Wenn die Installation unter dem System-Benutzerkonto ausgeführt wird, werden die Gruppen nur auf dem Administrationsserver erstellt.

Die Gruppen **KLAdmins** und **KLOperators** lassen sich mit den Standard-Administrationsfunktionen des Betriebssystems anzeigen. Mit denselben Funktionen können erforderliche Änderungen an den Benutzerrechten der Gruppen **KLAdmins** und **KLOperators** vorgenommen werden.

Die Gruppe **KLAdmins** verfügt über alle Berechtigungen, die Gruppe **KLOperators** nur über die Berechtigungen Lesen und Ausführen. Die Rechte der Gruppe **KLAdmins** dürfen nicht geändert werden.

Die Benutzer, die zur Gruppe **KLAdmins** gehören, werden als *Kaspersky Security Center Administratoren* bezeichnet, die Benutzer aus der Gruppe **KLOperators** werden als *Kaspersky Security Center Operatoren* bezeichnet.

Neben den Benutzern, die zur Gruppe **KLAdmins** gehören, werden die Administratorrechte von Kaspersky Security Center lokalen Administratoren von Geräten vergeben, auf denen der Administrationsserver installiert ist.

Sie können lokale Administratoren aus der Liste der Benutzer ausschließen, die über die Rechte des Kaspersky Security Center Administrators verfügen.

Alle Vorgänge, die von den Kaspersky Security Center Administratoren gestartet werden, werden mit den Rechten des Administrationsserver-Benutzerkontos ausgeführt.

Für jeden Administrationsserver im Netzwerk können Sie die einzelne Gruppe **KLAdmins** erstellen, die über die Rechte für die Arbeit nur mit diesem Server verfügt.

Wenn Geräte einer Domäne zu Administrationsgruppen verschiedener Server gehören, ist der Administrator der Domäne im Rahmen aller dieser Administrationsgruppen gleichzeitig Kaspersky Security Center Administrator. Die Gruppe **KLAdmins** ist dabei für diese Administrationsgruppen einheitlich und wird bei der Installation des ersten Administrationsservers angelegt. Vorgänge, die vom Kaspersky Security Center Administrator gestartet werden, werden mit den Rechten des Benutzerkontos des Administrationsservers ausgeführt, für den sie gestartet wurden.

Nach der Programminstallation kann der Kaspersky Security Center Administrator folgende Aktionen ausführen:

- Rechte ändern, welche an die Gruppen **KLOperators** vergeben werden
- Zugriffsrechte auf die Kaspersky Security Center Funktionen anderen Benutzergruppen und bestimmten Benutzern gewähren, die auf dem Administrator-Arbeitsplatz registriert wurden
- Zugriffsrechte für Benutzer in jeder Administrationsgruppe bestimmen.

Der Administrator von Kaspersky Security Center kann Zugriffsrechte auf jede Administrationsgruppe oder auf andere Objekte des Administrationsservers separat im Abschnitt **Sicherheit** des Eigenschaftenfensters eines gewählten Objekts bestimmen.

Sie können Benutzeraktionen mit den Datenträgern über Ereignisse des Administrationsservers verfolgen. Einträge zu Ereignissen werden im Knoten **Administrationsserver** auf der Registerkarte **Ereignisse** angezeigt. Diese Ereignisse haben die Ereigniskategorie **Infomeldung**, die Ereignistypen beginnen mit dem Wort **Audit**.

Bedingungen für das Herstellen einer Internetverbindung mit dem Administrationsserver

Wenn sich der Administrationsserver an einem Remotestandort (außerhalb des Firmennetzwerks) befindet, werden die Client-Geräte via Internet mit diesem verbunden. Zum Herstellen einer Internetverbindung zwischen Geräten und dem Administrationsserver müssen folgende Bedingungen erfüllt sein:

- Der Remote-Administrationsserver benötigt eine externe IP-Adresse, wobei die Eingangsports 13000 und 14000 geöffnet sein müssen.
- Auf den Geräten müssen Administrationsagenten installiert sein.
- Bei der Installation des Administrationsagenten auf den Geräten muss die IP-Adresse des Remote-Administrationsservers angegeben werden. Wenn für die Installation ein Installationspaket verwendet wird, muss die externe IP-Adresse manuell in den Eigenschaften des Installationspaketes im Abschnitt **Einstellungen** eingegeben werden.
- Um Programme und Aufgaben eines Geräts mit dem Administrationsserver verwalten zu können, aktivieren Sie im Eigenschaftenfenster des Geräts im Abschnitt **Allgemein** das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**. Nachdem Sie das Kontrollkästchen aktiviert haben, warten Sie auf die Synchronisierung mit dem Remote-Gerät. Eine ununterbrochene Verbindung mit dem Administrationsserver wird für maximal 100 Client-Geräte zugleich unterstützt.

Um die Ausführung der Aufgaben zu beschleunigen, die vom Remote-Administrationsserver eingehen, können Sie auf dem Gerät den Port 15000 öffnen. In diesem Fall sendet der Administrationsserver zum Starten der Aufgabe über den Port 15000 ein spezielles Paket an den Administrationsagenten, ohne auf den Abschluss der Synchronisierung mit dem Gerät zu warten.

Geschützte Verbindung mit dem Administrationsserver einrichten

Der Datenaustausch zwischen Client-Geräten und dem Administrationsserver und die Herstellung einer Verbindung der Verwaltungskonsole mit dem Administrationsserver können per SSL-Protokoll (Secure Socket Layer) erfolgen. Das SSL-Protokoll identifiziert die miteinander agierenden Seiten, führt eine Verschlüsselung der Datenübertragung durch und schützt sie vor Veränderungen bei der Übertragung. Das SSL-Protokoll basiert auf der Authentifizierung der miteinander agierenden Stellen und die Datenverschlüsselung mit offenen Schlüsseln.

In diesem Abschnitt

Serverauthentifizierung beim Verbinden des Geräts

Beim ersten Verbindungsaufbau zwischen einem Gerät und dem Administrationsserver, empfängt der Administrationsagent auf dem Gerät eine Kopie des Administrationsserverzertifikats und speichert sie lokal.

> Bei einer lokalen Installation des Administrationsagenten auf einem Gerät können Sie das Zertifikat des Administrationsservers manuell wählen.

Anhand der empfangenen Zertifikatskopie werden die Berechtigungen und Rechte des Administrationsservers bei den nachfolgenden Verbindungen überprüft.

Zusätzlich fragt der Administrationsagent bei jeder Verbindung des Geräts mit dem Administrationsserver das Zertifikat des Administrationsservers ab und vergleicht es mit der lokalen Kopie. Wenn sie nicht übereinstimmen, kann der Administrationsserver nicht auf das Gerät zugreifen.

Authentifizierung des Servers beim Verbindungsaufbau mit der Verwaltungskonsole

Beim ersten Verbindungsaufbau zum Administrationsserver nach der Installation fragt die Verwaltungskonsole das Zertifikat des Administrationsservers ab und speichert seine Kopie lokal auf dem Administrator-Arbeitsplatz. Anhand der empfangenen Zertifikatskopie wird der Administrationsserver bei nachfolgenden Verbindungen mit der Verwaltungskonsole identifiziert.

Wenn das Zertifikat des Administrationsservers nicht mit der auf dem Administrator-Arbeitsplatz gespeicherten Zertifikatskopie übereinstimmt, werden von der Verwaltungskonsole eine Bestätigung der Verbindung zum Administrationsserver mit dem angegebenen Namen und ein neues Zertifikat angefordert. Nach der Verbindung speichert die Verwaltungskonsole die Kopie des neuen Zertifikats des Administrationsservers, die zur künftigen Identifizierung des Servers dient.

Zertifikat des Administrationsservers

Der Administrationsserver wird beim Verbindungsaufbau mit der Verwaltungskonsole und beim Datenaustausch mit den Geräten mit dem *Zertifikat des Administrationsservers* authentifiziert. Außerdem wird das Zertifikat für die Authentifizierung beim Herstellen einer Verbindung zwischen Hauptadministrationsservern und untergeordneten Administrationsservern verwendet.

Das Zertifikat des Administrationsservers wird bei der Installation der Komponente Administrationsserver automatisch angelegt und im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert gespeichert.

Das Zertifikat des Administrationsservers wird nur einmal bei der Installation des Administrationsservers angelegt. Sollte das Zertifikat des Administrationsservers verloren gehen, sind zu dessen Wiederherstellung eine Neuinstallation der Komponente Administrationsserver und eine Wiederherstellung der Daten erforderlich (s. Abschnitt "Verschieben ins Backup und Wiederherstellung der Daten des Administrationsservers" auf S. 399).

Verbindung mit dem Administrationsserver trennen

Um die Verbindung mit dem Administrationsserver zu trennen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten aus, der dem Administrationsserver entspricht, dessen Verbindung getrennt werden muss.

2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Vom Administrationsserver trennen** aus.

Administrationsserver zur Konsolenstruktur hinzufügen

Um der Konsolenstruktur einen Administrationsserver hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Programmhauptfenster von Kaspersky Security Center in der Konsolenstruktur den Knoten **Kaspersky Security Center** aus.

2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen **Neu** → **Administrationsserver** aus.

In der Konsolenstruktur wird dadurch ein Knoten mit dem Namen **Administrationsserver – <Gerätename> (<Nicht verbunden>)** erstellt, von dem aus Sie eine Verbindung zu einem beliebigen der im Netzwerk installierten Administrationsserver herstellen können.

Administrationsserver aus der Konsolenstruktur entfernen

Um einen Administrationsserver aus der Konsolenstruktur zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten aus, der dem zu entfernenden Administrationsserver entspricht.

2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Entfernen** aus.

Benutzerkonto des Administrationsserver-Dienstes wechseln. Tool klsrvswch

Wenn es erforderlich ist, das Benutzerkonto des Administrationsserver-Dienstes zu wechseln, das bei der Installation von Kaspersky Security Center vorgegeben wurde, können Sie das Tool zum Wechseln des Administrationsserver-Benutzerkontos klsrvswch verwenden.

Bei der Installation von Kaspersky Security Center wird das Tool automatisch in den Installationsordner des Programms kopiert.

Das Tool kann beliebig oft gestartet werden.

Um das Administrationsserver-Benutzerkonto zu wechseln, gehen Sie wie folgt vor:

1. Starten Sie das Tool klsrvswch aus dem Installationsordner von Kaspersky Security Center.

   Daraufhin wird der Assistent zum Wechseln des Administrationsserver-Benutzerkontos gestartet. Folgen Sie den Anweisungen.

2. Wählen Sie im Fenster **Benutzerkonto für Dienst des Administrationsservers** eine der zwei Möglichkeiten zum Festlegen des Benutzerkontos:

   - **System-Benutzerkonto**. Der Dienst des Administrationsservers wird unter dem Benutzerkonto und mit den Rechten *System-Benutzerkonto* gestartet.

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

- **Benutzerkonto**: Der Dienst des Administrationsservers wird unter dem Benutzerkonto gestartet, das zur Domäne gehört. In diesem Fall initiiert der Administrationsserver alle Vorgänge mit den Rechten dieses Benutzerkontos.

  Um einen Benutzer auszuwählen, unter dessen Benutzerkonto der Dienst des Administrationsservers gestartet werden soll, gehen Sie wie folgt vor:

  1. Klicken Sie auf **Suchen**, und wählen Sie im folgenden Fenster **Auswahl: "Benutzer"** den erforderlichen Benutzer aus.

     Schließen Sie das Fenster **Auswahl: "Benutzer"**, und klicken Sie auf **Weiter**.

  2. Legen Sie bei Bedarf im Fenster **Kennwort des Benutzerkontos** ein Kennwort für das Benutzerkonto des gewählten Benutzers fest.

Nach Fertigstellung des Assistenten wird das Benutzerkonto des Administrationsservers geändert.

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.

Einstellungen des Administrationsservers anzeigen und ändern

Sie können die Einstellungen des Administrationsservers in seinem Eigenschaftenfenster anpassen.

Um das Eigenschaftenfenster des Administrationsserver zu öffnen,

klicken Sie mit der rechten Maustaste auf den Knoten des Administrationsservers und wählen Sie **Eigenschaften** aus.

In diesem Abschnitt

Allgemeine Einstellungen des Administrationsservers konfigurieren

Sie können allgemeine Einstellungen des Administrationsservers in den Abschnitten **Allgemein**, **Einstellungen**, **Ereignisse speichern** und **Sicherheit** im Eigenschaftenfenster des Administrationsservers anpassen.

Der Abschnitt **Sicherheit** kann nicht im Eigenschaftenfenster des Administrationsservers angezeigt werden, wenn die Anzeige in der Benutzeroberfläche der Verwaltungskonsole deaktiviert ist.

*Um die Ansicht des Abschnitts **Sicherheit** in der Verwaltungskonsole zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Programmhauptfenster im Menü **Ansicht** den Punkt **Benutzeroberfläche anpassen**.

2. Aktivieren Sie im folgenden Fenster **Benutzeroberfläche anpassen** das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** und klicken Sie auf die Schaltfläche **OK**.

3. Klicken Sie im Fenster mit den Programmmeldungen auf die Schaltfläche **OK**.

Der Abschnitt **Sicherheit** wird im Eigenschaftenfenster des Administrationsservers angezeigt.

Ereignisse auf dem Administrationsserver verarbeiten und speichern

Die Informationen über die Ausführung des Programms und der verwalteten Geräte werden in der Datenbank des Administrationsservers gespeichert. Jedes Ereignis gehört einem bestimmten Typ und einer Ereigniskategorie (Kritisches Ereignis, Funktionsfehler, Warnung, Infomeldung) an. Abhängig von den Umständen, unter denen das Ereignis aufgetreten ist, können Ereignissen eines Typs vom Programm verschiedene Ereigniskategorien zugeordnet werden.

Die Typen und Ereigniskategorien können Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignisbenachrichtigung** anzeigen. Ferner können Sie im Abschnitt **Ereignisbenachrichtigung** die Einstellungen für die Verarbeitung der einzelnen Ereignisse durch den Administrationsserver anpassen:

- Ereignisse auf dem Administrationsserver und in den Ereignisprotokollen des Betriebssystems auf dem Gerät und auf dem Administrationsserver erfassen

- Benachrichtigungsmethode des Administrators über die Ereignisse (beispielsweise SMS, E-Mail-Nachricht).

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignisse speichern** die Einstellungen für das Speichern der Ereignisse in der Datenbank des Servers anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Standardmäßig umfasst die Datenbank

des Administrationsservers 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 15.000.000 Ereignissen. Wenn die Anzahl der Ereignisse in der Datenbank den vom Administrator angegebenen Maximalwert erreicht, werden die ältesten Ereignisse vom Programm gelöscht und durch neue überschrieben.

Eintreten von Virenepidemien kontrollieren

Mit Kaspersky Security Center können Sie rechtzeitig auf Virenepidemien reagieren. Die Gefahr einer Virenepidemie wird durch die Kontrolle der Virenaktivität auf den Geräten eingeschätzt.

Sie können Regeln zum Einschätzen der Gefahr einer Virenepidemie und Aktionen, die im Falle einer Virenepidemie ausgeführt werden sollen, im Abschnitt **Virenangriff** des Administrationsserver-Eigenschaftenfensters anpassen.

Die Reihenfolge der Benachrichtigung über das Ereignis *Virenangriff* können Sie im Abschnitt **Ereignisbenachrichtigung** des Eigenschaftenfensters des Administrationsservers (s. Abschnitt "Ereignisse auf dem Administrationsserver verarbeiten und speichern" auf S. 106) im Eigenschaftenfenster des Ereignisses *Virenangriff* bestimmen.

Das Ereignis *Virenangriff* wird bei Eintritt des Ereignisses *Schädliches Objekt gefunden* während der Ausführung der Schutzsoftware gemeldet. Deshalb ist es erforderlich, Informationen über die Ereignisse *Schädliches Objekt gefunden* auf dem Administrationsserver zu speichern, um die Virenepidemie rechtzeitig erkennen zu können.

Die Einstellungen für das Speichern von Informationen über das Ereignis *Schädliches Objekt gefunden* werden in den Richtlinien der Schutzsoftware vorgegeben.

> Beim Zählen der Ereignisse *Schädliches Objekt gefunden* werden nur Informationen von den Geräten des Hauptadministrationsservers berücksichtigt.
> Informationen von untergeordneten Administrationsservern werden nicht berücksichtigt.
> Für jeden untergeordneten Server müssen die Einstellungen für das Ereignis *Virenangriff* individuell angepasst werden.

Datenverkehr begrenzen

Um den Netzwerkdatenverkehr zu reduzieren, können Sie die Geschwindigkeit der Datenübertragung von einzelnen IP-Bereichen und IP-Intervallen an den Administrationsserver einschränken.

Sie können Regeln für die Einschränkung des Datenverkehrs im Abschnitt **Datenverkehr** des Administrationsserver-Eigenschaftenfensters erstellen und anpassen.

Webserver-Einstellungen anpassen

Der Webserver ermöglicht die Veröffentlichung von autonomen Installationspaketen, iOS MDM-Profilen sowie Dateien aus dem freigegebenen Ordner.

Sie können die Einstellungen für die Verbindung des Webservers mit dem Administrationsserver anpassen und das Webserver-Zertifikat im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers festlegen.

Arbeit mit internen Benutzern

Die Benutzerkonten der *internen Benutzer* werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Unter dem Benutzerkonto eines internen Benutzers kann der Administrator eines virtuellen Servers die Kaspersky Security Center 10 Web Console starten, um sich Informationen über den Status der Antiviren-Sicherheit des Netzwerks anzeigen zu lassen. Innerhalb der Funktionen von Kaspersky Security Center verfügen die internen Benutzer über die Berechtigungen tatsächlicher Benutzer.

Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

Sie können die Benutzerkonto-Einstellungen für die internen Benutzer im Ordner **Benutzerkonten** de Konsolenstruktur (s. Abschnitt "Arbeiten mit Benutzerkonten" auf S. 179) anpassen.

Administrationsgruppen verwalten

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsgruppen.

Sie können mit den Administrationsgruppen folgende Aktionen ausführen:

- eine beliebige Anzahl von untergeordneten Gruppen aller Hierarchieebenen zu einer Administrationsgruppe hinzufügen
- Geräte zu Administrationsgruppen hinzufügen
- Hierarchie der Administrationsgruppen durch Verschieben einzelner Geräte und ganzer Gruppen in andere Gruppen ändern
- Untergruppen und Geräte aus Administrationsgruppen löschen
- dem Verzeichnis der Administrationsgruppen untergeordnete und virtuelle Administrationsserver hinzufügen
- Geräte aus Administrationsgruppen eines Servers in die Administrationsgruppen eines anderen Servers verschieben
- Festlegen, welche Kaspersky Lab-Programme automatisch auf den Geräten installiert werden sollen, die in eine Gruppe aufgenommen werden.

In diesem Abschnitt

Administrationsgruppen anlegen

Die Hierarchie der Administrationsgruppen wird im Programmhauptfenster von Kaspersky Security Center im Ordner **Verwaltete Geräte** erstellt. Die Administrationsgruppen werden als Ordner in der Konsolenstruktur angezeigt (s. Abb. unten).

Sofort nach der Installation von Kaspersky Security Center enthält der Ordner **Verwaltete Geräte** nur den leeren Ordner **Administrationsserver**.

> Ob der Ordner **Administrationsserver** in der Konsolenstruktur vorhanden ist, wird durch die Einstellungen der Benutzeroberfläche definiert. Um die Anzeige dieses Ordners zu aktivieren, wechseln Sie in das Menü **Ansicht** → **Benutzeroberfläche anpassen**, und aktivieren Sie im Fenster **Benutzeroberfläche anpassen** das Kontrollkästchen **Untergeordnete Administrationsserver anzeigen**.

Beim Erstellen einer Hierarchie der Administrationsgruppen können Sie zum Ordner **Verwaltete Geräte** Geräte, virtuelle Maschinen und untergeordnete Gruppen hinzufügen. Dem Ordner **Administrationsserver** können Sie untergeordnete Administrationsserver hinzufügen.

Jeder erstellte Gruppe enthält zunächst (auch wie der Ordner **Verwaltete Geräte**) den leeren Ordner **Administrationsserver**, der für die Arbeit mit den untergeordneten Administrationsservern der entsprechenden Gruppe vorgesehen ist. Informationen zu den Richtlinien, den Aufgaben einer bestimmten Gruppe sowie den dieser Gruppe gehörenden Geräten werden auf den entsprechenden Registerkarten im Arbeitsplatz dieser Gruppe angezeigt.

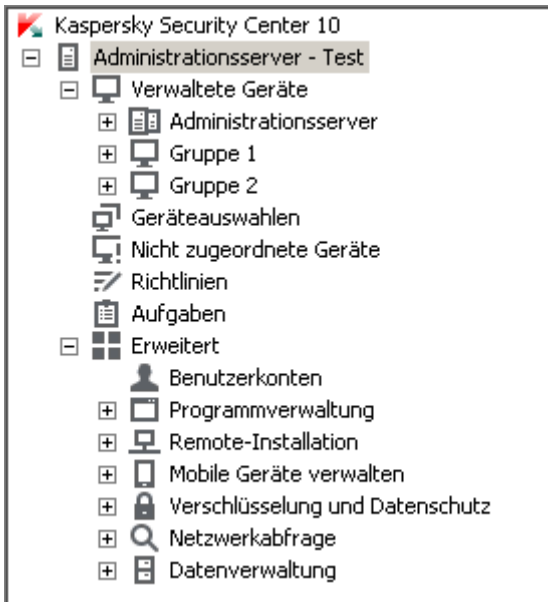


Abbildung 9. Hierarchie der Administrationsgruppen erstellen

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.

2. Wenn Sie eine untergeordnete Gruppe für eine vorhandene Administrationsgruppe erstellen möchten, wählen Sie im Ordner **Verwaltete Geräte** den Unterordner, welcher der Gruppe entspricht, zu der die neue Administrationsgruppe gehören soll.

   Wenn Sie eine neue Administrationsgruppe der obersten Hierarchieebene erstellen, können Sie diesen Schritt überspringen.

3. Starten Sie den Vorgang zum Erstellen einer Administrationsgruppe auf eine der folgenden Weisen:

   - mit dem Kontextmenübefehl **Erstellen** → **Gruppe**

   - mit der Schaltfläche **Gruppe erstellen**, die sich im Arbeitsplatz des Programmhauptfensters auf der Registerkarte **Gruppen** befindet.

4. Geben Sie im folgenden Fenster **Gruppenname** den Namen der Gruppe ein, und klicken Sie auf **OK**.

   Daraufhin wird in der Konsolenstruktur ein neuer Ordner der Administrationsgruppe mit dem angegebenen Namen angezeigt.

Das Programm ermöglicht, die Gruppenstruktur der Administrationsgruppen auf der Grundlage der Struktur von Active Directory oder der Struktur des Domänennetzwerks zu erstellen. Darüber hinaus können Sie die Gruppenstruktur auch aus einer Textdatei erstellen.

Um die Struktur der Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.

2. Klicken Sie mit der rechten Maustaste auf den Ordner **Verwaltete Geräte** und wählen **Alle Aufgaben** → **Gruppenstruktur anlegen** aus.

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

Administrationsgruppen verschieben

Sie können untergeordnete Administrationsgruppen innerhalb der Hierarchie der Gruppen verschieben.

Die Administrationsgruppe wird zusammen mit allen Untergruppen, untergeordneten Administrationsservern, Geräten sowie Gruppenrichtlinien und -aufgaben verschoben. Es werden alle Einstellungen auf sie angewendet, die ihrer neuen Stellung in der Hierarchie der Administrationsgruppen entsprechen.

Der Gruppenname muss innerhalb einer Hierarchieebene einmalig sein. Wenn im Ordner, in den Sie die Administrationsgruppe verschieben, eine Gruppe mit dem gleichen Namen bereits vorhanden ist, ändern Sie den Namen der Gruppe vor dem Verschieben. Wenn Sie den Namen der zu verschiebenden Gruppe zuvor nicht geändert haben, wird dem Namen der Gruppe beim Verschieben die Endung _**<laufende Nummer>** (z.B. **(1)**, **(2)**) hinzugefügt.

Sie können den Namen der Gruppe **Verwaltete Geräte** nicht ändern, da der Ordner ein integraler Bestandteil der Verwaltungskonsole ist.

Um eine Gruppe in einen anderen Ordner der Konsolenstruktur zu verschieben, gehen Sie wie folgt vor:

1. Wählen Sie die zu verschiebende Gruppe in der Konsolenstruktur aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verschieben Sie die Gruppe mit dem Kontextmenü:
     1. Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie **Ausschneiden** aus.
     2. Klicken Sie danach mit der rechten Maustaste auf die Administrationsgruppe, in welche die gewählte Gruppe verschoben werden soll, und wählen Sie **Einfügen** aus.
   - Verwenden Sie das Programmhauptmenü, um die Gruppe zu verschieben:
     a. Wählen Sie im Hauptmenü **Aktion** → **Ausschneiden** aus.
     b. Wählen Sie danach in der Konsolenstruktur die Administrationsgruppe aus, in welche die gewählte Gruppe verschoben werden soll.
     c. Wählen Sie im Hauptmenü **Aktion** → **Einfügen** aus.
   - Verschieben Sie die Gruppe in eine andere Gruppe mit der Maus.

Administrationsgruppen löschen

Sie können eine Administrationsgruppe löschen, wenn sie keine untergeordneten Administrationsserver, untergeordneten Gruppen und Client-Geräte enthält und wenn für sie keine Aufgaben und Richtlinien erstellt wurden.

Bevor eine Administrationsgruppe gelöscht wird, ist es erforderlich, untergeordnete Administrationsserver, Gruppen und Client-Geräte daraus zu löschen.

Um eine Gruppe zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die erforderliche Administrationsgruppe aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie **Entfernen** aus.
   - Klicken Sie mit der rechten Maustaste auf das Hauptmenü des Programms und wählen **Aktion** → **Entfernen** aus.
   - Drücken Sie die **Entf**-Taste.

Administrationsgruppenstruktur automatisch anlegen

Kaspersky Security Center ermöglicht es, automatisch mithilfe des Assistenten für das Erstellen einer Gruppenstruktur eine Struktur der Administrationsgruppen zu erstellen.

Der Assistent erstellt eine Struktur der Administrationsgruppen auf Grundlage folgender Daten:

- Domänenstruktur und Struktur der Arbeitsgruppen des Windows-Netzwerks
- Gruppenstruktur des Active Directory
- Inhalt einer Textdatei, die vom Administrator manuell erstellt wurde.

Beim Erstellen einer Textdatei sind folgende Regeln einzuhalten:

- Der Name jeder neuen Gruppe beginnt in einer neuen Zeile. Das Trennungszeichen ist der Zeilenumbruch. Leere Zeilen werden ignoriert.

Beispiel:

Büro 1

Büro 2

Büro 3

In der Zielgruppe werden drei Gruppen der ersten Hierarchieebene angelegt.

- Der Name der eingebetteten Gruppe muss hinter dem Schrägstrich (/) eingegeben werden.

Beispiel:

Büro 1/Untereinheit 1/Abteilung 1/Gruppe 1

In der Zielgruppe werden vier zueinander eingebettete Untergruppen angelegt.

- Um mehrere eingebettete Gruppen einer Hierarchieebene anzulegen, muss ein "vollständiger Pfad zur Gruppe" eingegeben werden.

Beispiel:

Büro 1/Untereinheit 1/Abteilung 1

Büro 1/Untereinheit 2/Abteilung 1

Büro 1/Untereinheit 3/Abteilung 1

Büro 1/Untereinheit 4/Abteilung 1

In der Zielgruppe wird eine Gruppe der ersten Hierarchieebene "Büro 1" angelegt, zu der vier eingebettete Gruppen einer Hierarchieebene "Untereinheit 1", "Untereinheit 2", "Untereinheit 3", "Untereinheit 4" gehören. Zu jeder Gruppe gehört eine Gruppe "Abteilung 1".

Das Erstellen der Administrationsgruppenstruktur mit dem Assistenten verletzt die Integrität des Netzwerks nicht: Neue Gruppen werden hinzugefügt, ersetzen aber nicht die vorhandenen Gruppen. Ein Client-Gerät kann zu einer Administrationsgruppe nicht erneut hinzugefügt werden, weil das Gerät beim Verschieben in die Administrationsgruppe aus der Gruppe **Nicht zugeordnete Geräte** gelöscht wird.

> Wenn beim Anlegen der Gruppenstruktur ein Gerät aus einem beliebigen Grund in der Gruppe **Nicht zugeordnete Geräte** nicht aufgenommen wird (ausgeschaltet, vom Netzwerk getrennt), dann wird es zur Administrationsgruppe nicht automatisch hinzugefügt. Sie können Geräte zu Administrationsgruppen manuell nach Abschluss des Assistenten hinzufügen.

Um das automatische Erstellen einer Administrationsgruppe zu starten, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Verwaltete Geräte** und wählen **Alle Aufgaben** → **Gruppenstruktur anlegen** aus.

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

Programme automatisch auf Geräten einer Administrationsgruppe installieren

Sie können angeben, welche Installationspakete für die automatische Remote-Installation von Kaspersky Lab-Programmen auf neu in die Gruppe aufgenommenen Client-Geräten verwendet werden sollen.

Um die automatische Installation von Anwendungen auf neuen Geräten in einer Administrationsgruppe zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die gewünschte Administrationsgruppe aus.

2. Öffnen Sie das Eigenschaftenfenster dieser Administrationsgruppe.

3. Wählen Sie im Abschnitt **Automatische Installation** die Installationspakete aus, die auf neuen Geräten installiert werden sollen, indem Sie die Kontrollkästchen neben den Namen der Installationspakete für gewünschte Programme aktivieren. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin werden Gruppenaufgaben angelegt, die auf den Client-Geräten gestartet werden, direkt nachdem diese zu der entsprechenden Administrationsgruppe hinzugefügt wurden.

Wenn für die automatische Installation mehrere Installationspakete einer Anwendung angegeben wurden, wird die Installationsaufgabe nur für die neueste Version der Anwendung erstellt.

Remote-Administration der Programme

Dieser Abschnitt enthält Informationen über die Remote-Verwaltung der auf den Client-Geräten installierten Programme von Kaspersky Lab mithilfe von Richtlinien, Richtlinienprofilen, Aufgaben und lokalen Programmeinstellungen.

In diesem Abschnitt

Richtlinienverwaltung

Die zentrale Konfiguration der Einstellungen für die Programme, die auf den Client-Geräten installiert sind, erfolgt über Richtlinien.

Die Richtlinien, die für die Programme in der Administrationsgruppe erstellt wurden, werden auf der Registerkarte **Richtlinien** im Arbeitsplatz angezeigt. Vor dem Namen jeder Richtlinie steht ein Symbol, mit dem der jeweilige Status angezeigt wird (s. Abschnitt "Statusmeldungen der Geräte, Aufgaben und Richtlinien" auf S. 430).

Nach Löschen der Richtlinie oder Außerkraftsetzung setzt das Programm die Arbeit mit den Einstellungen fort, die in der Richtlinie angegeben sind. Sie können diese Einstellungen später manuell ändern.

Die Richtlinie wird auf eine der folgenden Weisen übernommen: Wenn auf dem Gerät Echtzeitschutz-Aufgaben ausgeführt werden, werden bei der Ausführung der Aufgaben neue Einstellungen verwendet. Regelmäßige Aufgaben (Untersuchung auf Befehl, Datenbanken-Update) werden mit den unveränderten Einstellungen ausgeführt. Der nächste Start regelmäßiger Aufgaben erfolgt mit den geänderten Einstellungen.

Bei einer hierarchischen Struktur der Administrationsserver empfangen die untergeordneten Server Richtlinien vom Hauptadministrationsserver und verteilen sie auf die Client-Geräte. Ist die Vererbung aktiviert, lassen sich die Richtlinieneinstellungen auf dem Hauptadministrationsserver ändern. Nach dieser Änderung werden die Richtlinien, die auf die Einstellungen übernommen wurden, auf die vererbten Richtlinien auf den untergeordneten Administrationsservern übernommen.

Sollte die Verbindung zwischen Hauptadministrationsserver und untergeordneten Administrationsservern getrennt werden, gilt die Richtlinie auf dem untergeordneten Server mit den vorangegangenen Einstellungen weiter. Die auf dem Hauptadministrationsserver geänderten Richtlinieneinstellungen werden nach Wiederherstellung der Verbindung auf den untergeordneten Server übertragen.

Ist die Vererbung deaktiviert, lassen sich die Richtlinieneinstellungen auf dem untergeordneten Server ändern, und zwar unabhängig vom Hauptserver.

Wird die Verbindung zwischen Administrationsserver und Client-Gerät getrennt, tritt auf dem Gerät die mobile Richtlinie in Kraft (wenn definiert) oder es gilt die Richtlinie mit den vorangegangenen Einstellungen weiter bis zur Wiederherstellung der Verbindung.

Die Ergebnisse für die Verteilung der Richtlinie auf die untergeordneten Administrationsserver werden im Eigenschaftenfenster der Richtlinie auf dem Hauptadministrationsserver dargestellt.

Die Ergebnisse der Verteilung der Richtlinie auf die Client-Geräte werden im Eigenschaftenfenster der Richtlinie des Administrationsservers angezeigt, mit dem die Client-Geräte verbunden sind.

In diesem Abschnitt

Richtlinie anlegen

In der Verwaltungskonsole können Richtlinien unmittelbar im Ordner der Administrationsgruppe, für den die Richtlinie erstellt wird, und im Arbeitsplatz des Ordners **Richtlinien** erstellt werden.

Um eine Richtlinie im Ordner einer Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für welche die Richtlinie erstellt werden soll.

2. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien** aus.

3. Starten Sie mithilfe der Schaltfläche **Richtlinie erstellen** den Assistenten für das Erstellen einer Richtlinie.

Daraufhin wird der Assistent für das Erstellen einer Richtlinie gestartet. Folgen Sie den Anweisungen.

*Um eine Richtlinie im Arbeitsplatz des Ordners **Richtlinien** zu erstellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Starten Sie mithilfe der Schaltfläche **Richtlinie erstellen** den Assistenten für das Erstellen einer Richtlinie.

Daraufhin wird der Assistent für das Erstellen einer Richtlinie gestartet. Folgen Sie den Anweisungen.

In der Gruppe lassen sich für eine Anwendung mehrere Richtlinien erstellen, von denen aber immer nur eine Richtlinie aktiv sein kann. Beim Erstellen einer neuen, aktiven Richtlinie wird die vorangegangene aktive Richtlinie inaktiv.

Beim Erstellen einer Richtlinie können Sie Minimaleinstellungen anpassen, die für die Ausführung des Programms notwendig sind. Die übrigen Einstellungen behalten die Standardwerte und stimmen mit den Standardwerten bei der lokalen Anwendungsinstallation überein. Sie können die Richtlinie nach dem Erstellen ändern.

Einstellungen von Kaspersky Lab-Programmen, die nach der Richtlinienübernahme geändert werden, werden in entsprechenden Handbüchern ausführlich beschrieben.

Nach dem Erstellen der Richtlinie treten die Einstellungen, deren Änderung verboten ist (Schloss-Symbol ), auf den Client-Geräten in Kraft, unabhängig davon, welche Einstellungen für das Programm zuvor festgelegt wurden.

Vererbte Richtlinie in der untergeordneten Gruppe darstellen

Um die Anzeige einer vererbten Richtlinie für eine untergeordnete Administrationsgruppe zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für welche die vererbten Richtlinien angezeigt werden sollen.

2. Wählen Sie im Arbeitsplatz der gewählten Gruppe die Registerkarte **Richtlinien** aus.

3. Klicken Sie mit der rechten Maustaste auf die Richtlinienliste und wählen **Ansicht** → **Geerbte Richtlinien**.

Daraufhin werden die geerbten Richtlinien mit dem Symbol in der Richtlinienliste angezeigt.

-  – Wenn sie von der Gruppe vererbt wurden, die auf dem Hauptadministrationsserver erstellt wurde

- .  – Wenn sie von der Gruppe der obersten Ebene vererbt wurden.

Wenn der Modus zum Vererben von Einstellungen aktiviert ist, können die vererbten Richtlinien nur in der Gruppe geändert werden, in der sie erstellt wurden. Die vererbten Richtlinien können nicht in der Gruppe geändert werden, welche die Richtlinien geerbt hat.

Richtlinien aktivieren

Um eine Richtlinie für die gewählte Gruppe zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz der Gruppe auf der Registerkarte **Richtlinien** die Richtlinie aus, die aktiviert werden soll.

2. Zur Aktivierung der Richtlinie gehen Sie auf eine der folgenden Weisen vor:

   - Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Aktive Richtlinie** aus.

   - Öffnen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Allgemein**, und wählen Sie in der Einstellungsgruppe **Richtlinienstatus** die Option **Aktive Richtlinie** aus.

Daraufhin wird die Richtlinie für die gewählte Administrationsgruppe aktiviert.

Wenn die Richtlinie eine Weile auf einer großen Anzahl von Client-Geräten angewendet wird, erhöhen sich die Belastung für den Administrationsserver und der Umfang des Datenverkehrs im Netzwerk erheblich.

Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren

Damit eine Richtlinie beim Eintritt eines Ereignisses automatisch aktiviert wird, gehen Sie wie folgt vor:

1. Öffnen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Virenangriff**.

2. Öffnen Sie danach mit dem Link **Aktivierung der Richtlinien nach Ereignis "Virenangriff" einstellen** das Fenster **Aktivierung von Richtlinien**, und fügen Sie der von Ihnen gewählten Liste der Richtlinien, die beim Erkennen eines Virenangriffs aktiviert werden, die Richtlinie hinzu.

Wird eine Richtlinie nach dem Ereignis *Virenangriff* aktiviert, kann zu der vorangegangenen Richtlinie nur manuell zurückgekehrt werden.

Mobile Richtlinie übernehmen

Die mobile Richtlinie tritt auf einem Gerät in Kraft, wenn das Gerät vom Firmennetzwerk getrennt wird.

Um eine gewählte mobile Richtlinie zu übernehmen,

öffnen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Allgemein**, und wählen Sie in der Einstellungsgruppe **Richtlinienstatus** die Option **Mobile Richtlinie** aus.

Dann tritt die Richtlinie auf den Geräten in Kraft, wenn sie vom Firmennetzwerk getrennt werden.

Richtlinie ändern. Rollback der Änderungen

Um eine Richtlinie zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie im Arbeitsplatz des Ordners **Richtlinien** die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
3. Nehmen Sie die notwendigen Änderungen vor.
4. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie, im Abschnitt **Revisionsverlauf** gespeichert.

Notfalls können Sie die Änderungen der Richtlinie zurücksetzen.

Um die Änderungen einer Richtlinie zurückzusetzen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Richtlinien** aus.
2. Wählen Sie die Richtlinie, deren Änderungen zurückgesetzt werden sollen, aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
3. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Revisionsverlauf** aus.

4. Wählen Sie in der Liste mit den Richtlinienrevisionen die Nummer der Revision aus, deren Änderungen zurückgesetzt werden sollen.

5. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Rollback**.

Richtlinien löschen

Um eine Richtlinie zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz der Administrationsgruppe auf der Registerkarte **Richtlinien** die Richtlinie aus, die gelöscht werden soll.

2. Löschen Sie die Richtlinie auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Entfernen** aus.

   - Klicken Sie im Arbeitsplatz der gewählten Richtlinie auf den Link **Richtlinie löschen**.

Richtlinien kopieren

Um eine Richtlinie zu kopieren, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz der gewünschten Gruppe auf der Registerkarte **Richtlinien** die entsprechende Richtlinie aus.

2. Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Kopieren** aus.

3. Wählen Sie in der Konsolenstruktur die Gruppe aus, zu der die Richtlinie hinzugefügt werden soll.

   Die Richtlinie kann zur selben Gruppe hinzugefügt werden, aus der sie kopiert wurde.

4. Klicken Sie mit der rechten Maustaste auf die Richtlinienliste für die gewählte Gruppe auf der Registerkarte **Richtlinien** und wählen Sie **Einfügen** aus.

Daraufhin wird die Richtlinie mit allen Einstellungen kopiert und auf alle Geräte der Gruppe verteilt, auf die sie übertragen wurde. Wenn Sie die Richtlinie in dieselbe Gruppe einfügen, von der sie kopiert wurde, wird dem Namen der Richtlinie automatisch die Endung der Form **(<laufende Nummer>)** hinzugefügt. Beispiel: **(1)**, **(2)**.

Eine aktive Richtlinie wird nach dem Kopieren inaktiv. Sie können bei Bedarf die Richtlinie aktivieren.

Richtlinien exportieren

Um eine Richtlinie zu exportieren, gehen Sie wie folgt vor:

1. Exportieren Sie die Richtlinie auf eine der folgenden Weisen:
   - Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen **Alle Aufgaben** → **Exportieren** aus.
   - Klicken Sie im Arbeitsplatz der Richtlinie auf den Link **Richtlinie in Datei exportieren**.
2. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Richtliniendatei zum Speichern an. Klicken Sie auf **Speichern**.

Richtlinien importieren

Um eine Richtlinie zu importieren, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz der gewünschten Gruppe auf der Registerkarte **Richtlinien** eine der folgenden Methoden für den Import der Richtlinie aus:
   - Klicken Sie mit der rechten Maustaste auf die Richtlinienliste und wählen **Alle Aufgaben** → **Importieren** aus.
   - Klicken Sie im Block zur Verwaltung der Richtlinienliste auf den Link **Richtlinie aus Datei importieren**.
2. Geben Sie im folgenden Fenster den Pfad zu der Datei an, aus der Sie die Richtlinie importieren wollen. Klicken Sie auf **Öffnen**.

Daraufhin wird die hinzugefügte Richtlinie in der Richtlinienliste angezeigt.

Wenn in der gewählten Richtlinienliste eine Richtlinie mit dem gleichen Namen wie die zu importierende Richtlinie bereits vorhanden ist, wird dem Namen der zu importierenden Richtlinie eine Endung der Form **(<laufende Nummer>)** angehängt. Beispiel: **(1)**, **(2)**.

Richtlinien konvertieren

Kaspersky Security Center ermöglicht es, die Richtlinien vorheriger Versionen der Kaspersky-Lab-Programme in die Richtlinien aktueller Versionen dieser Programme zu konvertieren.

Die Konvertierung von Richtlinien ist nur für die folgenden Programme möglich:

- Kaspersky Anti-Virus 6.0 für Windows Workstation MP4
- Kaspersky Endpoint Security 8 für Windows
- Kaspersky Endpoint Security 10 für Windows.

Um Richtlinien konvertieren zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus, für den Richtlinien konvertiert werden sollen.
2. Wählen Sie im Kontextmenü des Administrationsservers den Punkt **Alle Aufgaben** → **Assistent für die Stapelkonvertierung von Richtlinien und Aufgaben**.

   Daraufhin wird der Assistent zum Konvertieren von Richtlinien und Aufgaben gestartet. Folgen Sie den Anweisungen.

Nach Fertigstellung des Assistenten werden neue Richtlinien erstellt, die die Einstellungen für die Richtlinien vorheriger Versionen von Kaspersky-Lab-Programmen verwenden.

Richtlinienprofile verwalten

Dieser Abschnitt enthält Informationen über Richtlinienprofile, die zur effektiven Verwaltung der Gruppen von Client-Geräten verwendet werden. Es werden die Vorteile der Richtlinienprofile sowie die Möglichkeiten ihrer Anwendung beschrieben. Ferner werden in diesem Abschnitt Anweisungen für die Erstellung und Löschung von Richtlinienprofilen angeführt.

Über Richtlinienprofile

Ein Richtlinienprofil ist eine benannte Auswahl von angewendeten Richtlinieneinstellungen, die bei der Erfüllung von bestimmten Bedingungen auf dem Client-Gerät (Computer, mobiles Gerät) aktiviert wird. Bei der Aktivierung des Profils werden die Einstellungen der bis zur Aktivierung des Profils auf dem Gerät geltenden Richtlinie geändert. Diese Einstellungen nehmen die im Profil festgelegten Werte an.

Die Profile werden nur für die folgenden Richtlinien unterstützt:

- Richtlinien des Programms Kaspersky Endpoint Security 10 Service Pack 1 für Windows und höher
- Richtlinien des Programms Kaspersky Endpoint Security 10 Service Pack 1 für Mac und höher
- Richtlinien des Plug-Ins für Kaspersky Mobile Device Management 10 Service Pack 1 und höher.

Vorteile von Richtlinienprofilen

Richtlinienprofile erleichtern die Verwaltung von Client-Geräten mithilfe von Richtlinien:

- Profile enthalten nur jene Einstellungen, die sich von der "Basisrichtlinie" unterscheiden.
- Es ist nicht erforderlich, manuell mehrere Kopien einer Richtlinie zu unterstützen und anzuwenden, wenn sich diese nur durch wenige Einstellungen unterscheiden.
- Es ist keine separate mobile Richtlinie erforderlich.

- Neue Richtlinien können problemlos erstellt werden, da der Export und Import von Profilen unterstützt wird, sowie neue Profile durch Kopieren von bestehenden Profilen erstellt werden können.
- Auf einem Client-Gerät können gleichzeitig mehrere Richtlinienprofile aktiv sein.
- Hierarchische Richtlinien werden unterstützt.

Aktivierungsregeln für Profile. Profilpriorität

Richtlinienprofile werden auf dem Client-Gerät mithilfe von Aktivierungsregeln aktiviert. Aktivierungsregeln können folgende Bedingungen enthalten:

- Der Administrationsagent auf dem Client-Gerät stellt unter Berücksichtigung bestimmter Verbindungseinstellungen, beispielsweise Serveradresse, Portnummer usw., eine Verbindung zum Server her.
- Das Client-Gerät befindet sich im autonomen Modus.
- Dem Client-Gerät sind bestimmte Tags zugewiesen.
- Das Client-Gerät befindet in einem bestimmten Unterverzeichnis von Active Directory®, das Gerät oder sein Eigentümer befindet sich in der Sicherheitsgruppe Active Directory.
- Das Client-Gerät gehört einem bestimmten Eigentümer oder der Eigentümer des Geräts befindet sich in einer internen Sicherheitsgruppe von Kaspersky Security Center.

Die für die Richtlinie erstellten Profile sind in absteigender Priorität gereiht. Wenn sich besitzt das Profil *X* in der Liste der Profile vor Profil *Y* befindet, dann hat Profil *X* eine höhere Priorität als *Y*. Die Priorität von Profilen ist zwingend erforderlich, da auf dem Client-Gerät gleichzeitig mehrere Profile aktiv sein können.

Richtlinien in hierarchischen Administrationsgruppen

Da sich Richtlinien gegenseitig entsprechend der Hierarchie der Administrationsgruppen beeinflussen, werden Profile mit demselben Namen zusammengeführt. Profile von "höheren" Richtlinien haben eine höhere Priorität. Beispielsweise umfasst die Richtlinie *P(A)* in der Administrationsgruppe *A* die Profile *X1*, *X2* und *X3* in absteigender Reihenfolge. In der Administrationsgruppe *B*, die eine Untergruppe von Gruppe *A* ist, wird die Richtlinie *P(B)* mit den Profilen *X2*, *X4* und *X5* erstellt. Somit wird die Richtlinie *P(B)* durch die Richtlinie *P(A)*

geändert, weil die Liste der Profile in der Richtlinie *P(B)* in absteigender Reihenfolge *X1*, *X2*, *X3*, *X4*, *X5* lautet. Die Priorität von Profile *X2* hängt vom ursprünglichen Status von *X2* in der Richtlinie *P(B)* und *X2* in der Richtlinie *P(A)* ab.

Die aktive Richtlinie ist die Summer aus Hauptrichtlinie und allen aktiven Profilen dieser Richtlinie, d. h. jener Profile, für die eine Aktivierungsregel ausgeführt wird. Die aktive Richtlinie wird beim Start des Administrationsagenten, bei der Aktivierung bzw.
Deaktivierung des autonomen Modus sowie bei einer Änderung der dem Client-Gerät zugewiesenen Tag-Liste neu berechnet.

Eigenschaften und Beschränkungen von Richtlinienprofilen

Profile haben folgende Eigenschaften:

- Profile von nicht aktiven Richtlinien haben keine Auswirkung auf Client-Geräte.
- Wenn eine Richtlinie im autonomen Modus aktiv ist, werden auch die Profile dieser Richtlinie nur im autonomen Modus angewendet.
- Die statistische Zugriffsanalyse auf ausführbare Dateien wird von Profilen nicht unterstützt.
- Eine Richtlinie darf keine Benachrichtigungseinstellungen enthalten.
- Wenn für die Verbindung des Geräts mit dem Administrationsserver der UDP-Port 15000 verwendet wird, muss das entsprechende Richtlinienprofil bei der Zuweisung eines Tags auf dem Gerät innerhalb von einer Minute aktiviert werden.
- Die Regeln für die Herstellung einer Verbindung zwischen Administrationsagent und Administrationsserver können bei der Erstellung von Aktivierungsregeln für Profile verwendet werden.

Richtlinienprofil erstellen

Profile können nur für Richtlinien von Kaspersky Endpoint Security 10 Service Pack 1 für Windows erstellt werden.

Um ein Richtlinienprofil für eine Administrationsgruppe anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Richtlinienprofil erstellt werden soll.
2. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Richtlinienprofil** und klicken Sie auf die Schaltfläche **Hinzufügen**.
5. Passen Sie im Fenster **Eigenschaften: Neues Profil** die Eigenschaften des Richtlinienprofils an:
   - Geben Sie im Abschnitt **Allgemein** den Namen des Profils an.

     Der Name des Profils darf nicht mehr als 100 Zeichen umfassen.
   - Aktivieren bzw. deaktivieren Sie das Profil mithilfe des Kontrollkästchens **Profil aktivieren**.

     Wenn das Kontrollkästchen deaktiviert ist, wird das Profil nicht zur Verwaltung des Geräts verwendet.
6. Erstellen Sie im Abschnitt **Aktivierungsregeln** die Aktivierungsregeln für das Profil:
   - Klicken Sie auf die Schaltfläche **Hinzufügen**.
   - Konfigurieren Sie die Aktivierungsregeln des Richtlinienprofils in Fenster **Eigenschaften: Neue Regel**.
   - Klicken Sie auf die Schaltfläche **OK**.

7. Ändern Sie die Einstellungen der Richtlinie in den entsprechenden Abschnitten.

8. Speichern Sie die Änderungen nach der Konfiguration des Profils und der Erstellung der Aktivierungsregeln mithilfe der Schaltfläche **OK**.

Das Profil wird gespeichert. Das Profil wird auf dem Gerät aktiviert, wenn die Aktivierungsregel ausgeführt wird.

Profile, die für eine Richtlinie erstellt wurden, werden in den Eigenschaften der Richtlinie im Abschnitt **Richtlinienprofile** angezeigt. Sie können ein Richtlinienprofil und die Priorität des Profils ändern (s. Abschnitt "Richtlinienprofil ändern" auf S. 132) sowie ein Profil entfernen (s. Abschnitt "Richtlinienprofil löschen" auf S. 134).

Bei der Ausführung der Aktivierungsregeln können mehrere Richtlinienprofile gleichzeitig aktiviert werden.

Richtlinienprofile ändern

Einstellungen eines Richtlinienprofils ändern

Profile können nur für Richtlinien von Kaspersky Endpoint Security 10 Service Pack 1 für Windows geändert werden.

Um die Einstellungen eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Richtlinienprofil geändert werden soll.

2. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien** aus.

3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.

4. Öffnen Sie in den Eigenschaften der Richtlinie den Abschnitt **Richtlinienprofil** aus.

   Dieser Abschnitt enthält eine Liste der für diese Richtlinie erstellten Profile. Die Profile werden in der Liste entsprechend ihrer Priorität angezeigt.

5. Wählen Sie ein Richtlinienprofil und klicken Sie auf die Schaltfläche **Eigenschaften**.

6. Passen Sie im Eigenschaftenfenster die Einstellungen des Profils an:

   - Ändern Sie im Abschnitt **Allgemein** erforderlichenfalls den Namen des Profils und aktivieren bzw. deaktivieren Sie das Profil mithilfe des Kontrollkästchens **Profil aktivieren**.

   - Ändern Sie im Abschnitt **Aktivierungsregeln** die Aktivierungsregeln für das Profil.

   - Ändern Sie die Einstellungen der Richtlinie in den entsprechenden Abschnitten.

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

Die geänderten Einstellungen werden nach der Synchronisierung des Geräts mit dem Administrationsserver (wenn das Richtlinienprofil aktiv ist) bzw. nach der Ausführung der Aktivierungsregeln (wenn das Richtlinienprofil nicht aktiv ist) angewendet.

Priorität eines Richtlinienprofils ändern

Durch die Priorität von Richtlinienprofilen wird die Aktivierungsreihenfolge der Profile auf dem Client-Gerät bestimmt. Die Priorität wird verwendet, wenn für verschiedene Richtlinienprofile die gleichen Aktivierungsregeln festgelegt sind.

Beispielsweise wurden die beiden Richtlinienprofile *Profil 1* und *Profil 2* erstellt, die sich voneinander durch den Wert einer Einstellung unterscheiden (*Wert 1* und *Wert 2*). Die Priorität von *Profil 1* ist höher als die Priorität von *Profil 2*. Außerdem existieren Profile mit einer niedrigeren Priorität als *Profil 2*. Die Aktivierungsregeln der Profile stimmen überein.

Bei der Ausführung der Aktivierungsregeln wird *Profil 1* aktiviert. Die Einstellung auf dem Gerät nimmt den *Wert 1* an. Wenn *Profil 1* gelöscht wird, erhält *Profil 2* die gleiche Priorität und die Einstellung nimmt den *Wert 2* an.

In der Liste der Richtlinienprofile werden die Profile entsprechend ihrer Priorität angezeigt. An erster Stelle der Liste steht das Profil mit der höchsten Priorität. Die Priorität der Profile kann mithilfe der Schaltflächen  und  geändert werden.

Richtlinienprofil löschen

Um ein Richtlinienprofil zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Richtlinienprofil entfernt werden soll.
2. Wählen Sie im Arbeitsplatz der Administrationsgruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Richtlinie.
4. Öffnen Sie in den Eigenschaften der Richtlinie für Kaspersky Endpoint Security den Abschnitt **Richtlinienprofil**.
5. Wählen Sie das zu löschende Richtlinienprofil und klicken Sie auf die Schaltfläche **Löschen**.

Das Richtlinienprofil wird gelöscht. Aktiv wird entweder ein anderes Richtlinienprofil, dessen Aktivierungsregeln auf dem Gerät ausgeführt werden, oder eine Richtlinie.

Aufgaben verwalten

Kaspersky Security Center verwaltet die auf Geräten installierten Programme durch das Erstellen und Starten von Aufgaben. Die Aufgaben ermöglichen Installation, Start und Beenden von Programmen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Programm-Module sowie Ausführung anderer Aktionen mit den Programmen.

Die Aufgaben werden in folgende Arten unterteilt:

- *Gruppenaufgaben*: Aufgaben, die auf den Geräten der gewählten Administrationsgruppe ausgeführt werden.
- *Aufgaben des Administrationsservers* Aufgaben, die auf dem Administrationsserver ausgeführt werden.

- *Aufgaben für bestimmte Geräte*: Aufgaben, die auf gewählten Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Administrationsgruppe gehören.
- *Lokale Aufgaben*: Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

Aufgaben für Programme lassen sich nur anlegen, wenn auf dem Administrator-Arbeitsplatz das Verwaltungs-Plug-in für dieses Programm installiert ist.

Zum Erstellen der Liste der Geräte, für die eine Aufgabe erstellt werden soll, können folgende Methoden angewandt werden:

- Geräte auswählen, die vom Administrationsserver im Netzwerk gefunden wurden.
- Geräteliste manuell erstellen Als Adresse des Geräts können Sie die IP-Adresse (oder das IP-Intervall), den NetBIOS- oder den DNS-Namen verwenden.
- Geräteliste aus einer TXT-Datei, die ein Verzeichnis hinzuzufügender Geräte enthält, importieren (jeweils nur eine Adresse pro Zeile).

  Wird die Geräteliste aus der Datei importiert oder manuell erstellt, während die Geräte namentlich identifiziert werden, so werden der Liste nur die Geräte hinzugefügt, deren Daten bereits infolge der Anbindung oder einer Netzwerkabfrage in der Datenbank des Administrationsservers vorhanden sind.

Sie können für jedes Programm eine beliebige Anzahl von Gruppenaufgaben, Aufgaben für bestimmte Geräte und lokalen Aufgaben erstellen.

Der Datenaustausch über die Aufgaben zwischen einem Programm auf dem Gerät und der Datenbank von Kaspersky Security Center erfolgt beim Verbindungsaufbau des Administrationsagenten mit dem Administrationsserver.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt einer Aufgabe verfolgen, Aufgaben kopieren, exportieren, importieren und löschen.

Aufgaben können auf einem Gerät nur dann gestartet werden, wenn das Programm gestartet wurde, für das diese Aufgaben erstellt worden waren. Beim Beenden einer Anwendung wird die Ausführung aller gestarteten Aufgaben abgebrochen.

Die Ergebnisse der Aufgabenausführung werden in den Ereignisprotokollen von Microsoft Windows und von Kaspersky Security Center zentral auf dem Administrationsserver und lokal auf jedem Gerät gespeichert.

Gruppenaufgaben erstellen

In der Verwaltungskonsole können Aufgaben unmittelbar im Ordner der Administrationsgruppe, für den die Gruppenaufgabe erstellt wird, und im Arbeitsplatz des Ordners **Aufgaben** erstellt werden.

Um eine Gruppenaufgabe im Ordner einer Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die eine Aufgabe erstellt werden soll.
2. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Aufgaben** aus.
3. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**, um die Erstellung der Aufgabe zu starten.

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

*Um eine Aufgabe im Arbeitsplatz des Ordners **Aufgaben** zu erstellen, gehen Sie wie folgt vor:*

1. Wahlen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**, um die Erstellung der Aufgabe zu starten.

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

Aufgaben des Administrationsservers erstellen

Der Administrationsserver führt folgende Aufgaben aus:

- Berichte automatisch versenden
- Updates in die Datenverwaltung herunterladen
- Sicherungskopie der Daten des Administrationsservers erstellen
- Datenbank bedienen
- Windows-Updates synchronisieren
- Installationspaket anhand des Betriebssystem-Abbilds eines Mustergeräts erstellen.

Auf dem virtuellen Administrationsserver sind nur die Aufgaben zum automatischen Versand von Berichten und zur Erstellung eines Installationspaketes anhand des Betriebssystem-Abbilds eines Mustergeräts verfügbar. In der Datenverwaltung des virtuellen Servers werden Updates angezeigt, die auf dem Haupt-Administrationsserver heruntergeladen wurden.
Das Verschieben von Daten des virtuellen Servers ins Backup wird im Rahmen der Erstellung einer Sicherungskopie der Daten des Hauptadministrationsservers ausgeführt.

Um eine Aufgabe für den Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:
   - Wählen Sie in der Konsolenstruktur aus dem Kontextmenü des Ordners **Aufgaben** den Punkt **Erstellen** → **Aufgabe**.
   - Mithilfe der Schaltfläche **Aufgabe erstellen** im Arbeitsplatz des Ordners **Aufgaben**.

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

Die Aufgaben **Herunterladen von Updates in die Datenverwaltung**, **Windows-Updates synchronisieren**, **Datenbank bedienen** und **Sicherungskopie der Serverdaten erstellen** lassen sich nur einmal anlegen. Wurden die Aufgaben **Herunterladen von Updates in die Datenverwaltung**, **Datenbank bedienen**, **Sicherungskopie der Serverdaten erstellen** und **Windows-Updates synchronisieren** für den Administrationsserver bereits erstellt, werden sie im Fenster zur Auswahl eines Aufgabentyps des Assistenten für das Erstellen von Aufgaben nicht mehr angezeigt.

Aufgabe für bestimmte Geräte erstellen

Kaspersky Security Center ermöglicht das Erstellen von Aufgaben für bestimmte Geräte nach freier Auswahl. Diese Geräte können zu unterschiedlichen Administrationsgruppen oder zu keiner Administrationsgruppe gehören. Kaspersky Security Center ermöglicht die Ausführung folgender Aufgaben für bestimmte Geräte:

- Remote-Installation eines Programms (weitere Details siehe: *Kaspersky Security Center Implementierungshandbuch*);
- Benutzernachricht (s. Abschnitt "Nachricht an Gerätenutzer senden" auf S. 167);
- Administrationsserver wechseln (s. Abschnitt "Administrationsserver für Client-Geräte wechseln" auf S. 164);
- Gerät verwalten (s. Abschnitt "Client-Geräte von einem entfernten Standort einschalten, ausschalten und Neustart durchführen" auf S. 166);
- Update-Prüfung (s. Abschnitt "Heruntergeladene Updates überprüfen" auf S. 338);
- Verteilung des Installationspakets (weitere Details siehe: *Kaspersky Security Center Implementierungshandbuch*);
- Remote-Installation eines Programms auf untergeordneten Administrationsservern (weitere Details siehe: *Kaspersky Security Center Implementierungshandbuch*);
- Remote-Deinstallation eines Programms (weitere Details siehe: *Kaspersky Security Center Implementierungshandbuch*).

Um eine Aufgabe für bestimmte Geräte zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.

2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:

   - Wählen Sie im Kontextmenü des Ordners **Aufgaben** der Konsolenstruktur den Punkt **Erstellen** → **Aufgabe** aus.

   - Mithilfe der Schaltfläche **Aufgabe erstellen** im Arbeitsplatz des Ordners **Aufgaben**.

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

Lokale Aufgabe erstellen

Um eine lokale Aufgabe für ein Gerät zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz der Gruppe, zu welcher das gewünschte Gerät gehört, die Registerkarte **Geräte** aus.

2. Wählen Sie in der Geräteliste auf der Registerkarte **Geräte** das Gerät aus, für das eine lokale Aufgabe erstellt werden soll.

3. Starten Sie den Vorgang zum Erstellen der Aufgabe für das gewählte Gerät auf eine der folgenden Weisen:

   - Klicken Sie auf die Schaltfläche **Aktion ausführen** und wählen Sie in der Dropdown-Liste die Option **Aufgabe erstellen**.

   - Durch Klicken auf den Link **Aufgabe erstellen** im Arbeitsplatz für das gewählte Gerät.

   - Im Eigenschaftenfenster des Geräts auf eine der folgenden Weisen:

     a. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.

     b. Wählen Sie im folgenden Eigenschaftenfenster des Geräts den Abschnitt **Aufgaben** aus, und klicken Sie auf **Hinzufügen**.

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

Eine ausführliche Beschreibung über das Erstellen und Konfigurieren der lokalen Aufgaben finden Sie in den Handbüchern der betreffenden Kaspersky-Lab-Programme.

Vererbte Gruppenaufgabe im Arbeitsbereich der untergeordneten Gruppe anzeigen

Um die Anzeige von geerbten Aufgaben für eine untergeordnete Gruppe im Arbeitsplatz zu aktivieren, gehen Sie wie folgt vor:

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

2. Klicken Sie im Arbeitsplatz der Registerkarte **Aufgaben** auf die Schaltfläche **Geerbte Aufgaben anzeigen**.

Daraufhin werden die geerbten Aufgaben mit dem Symbol in der Aufgabenliste angezeigt:

-  – Wenn sie von der Gruppe vererbt wurden, die auf dem Hauptadministrationsserver erstellt wurde

-  – Wenn sie von der Gruppe der obersten Ebene vererbt wurden.

Im Modus zum Vererben zur Bearbeitung von vererbten Aufgaben kann nur die Gruppe bearbeitet werden, in der sie erstellt wurden. Die geerbten Aufgaben können in der Gruppe, die die Aufgaben vererbt, nicht geändert werden.

Geräte vor Ausführung einer Aufgabe automatisch einschalten

Kaspersky Security Center ermöglicht, die Aufgabeneinstellungen so anzupassen, dass vor der Ausführung einer Aufgabe auf den ausgeschalteten Geräten das Betriebssystem hochgefahren wird.

Um das automatische Hochfahren von Geräten vor dem Aufgabenstart einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus.
2. Klicken Sie auf den Link **Erweitert**, um das Fenster zu öffnen, in dem Aktionen mit den Geräten angepasst werden.
3. Aktivieren Sie im Fenster **Erweitert** das Kontrollkästchen **Gerät vor dem Aufgabenstart per Wake on LAN aktivieren (Min.)**, und geben Sie die Zeit in Minuten ein.

Die daraufhin deaktivierten Geräte werden in der festgelegten Anzahl von Minuten bis zum Aufgabenstart automatisch aktiviert, und auf diesen Geräten wird das Betriebssystem geladen.

Das automatische Starten des Betriebssystems ist nur auf den Geräten mit Unterstützung der Funktion Wake On Lan verfügbar.

Gerät nach der Ausführung einer Aufgabe automatisch ausschalten

Kaspersky Security Center ermöglicht es, die Aufgabeneinstellungen so anzupassen, dass nach der Ausführung der Aufgabe diejenigen Geräte, auf denen sie ausgeführt wird, automatisch ausgeschaltet werden.

Damit Geräte nach der Ausführung der Aufgabe automatisch ausgeschaltet werden, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus.
2. Klicken Sie auf den Link **Erweitert**, um das Fenster zu öffnen, in dem Aktionen mit den Geräten angepasst werden.
3. Aktivieren Sie im Fenster **Erweitert** das Kontrollkästchen **Gerät nach Beendigung der Aufgabe herunterfahren**.

Zeitlimit für Aufgabenausführung festlegen

Um die Zeitdauer der Aufgabenausführung auf Geräten einzuschränken, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus.
2. Klicken Sie auf den Link **Erweitert**, um im folgenden Fenster Aktionen mit den Client-Geräten anzupassen.
3. Aktivieren Sie im Fenster **Erweitert** das Kontrollkästchen **Anhalten, wenn Aufgabe länger ausgeführt wird als (Min.)**, und geben Sie die Zeit in Minuten an.

Daraufhin wird die Ausführung der Aufgabe von Kaspersky Security Center automatisch abgebrochen, wenn nach Ablauf des angegebenen Zeitraums die Aufgabe nicht beendet wurde.

Aufgaben exportieren

Sie können Gruppenaufgaben und Aufgaben für bestimmte Geräte in eine Datei exportieren. Die Aufgaben des Administrationsservers und die lokalen Aufgaben sind für den Export nicht verfügbar.

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

1. Klicken Sie mit der rechten Maustaste auf die Aufgaben und wählen **Alle Aufgaben** → **Exportieren**.
2. Geben Sie im folgenden Fenster **Speichern unter** den Namen und Pfad der Datei zum Speichern an.
3. Klicken Sie auf **Speichern**.

Die Rechte der lokalen Administratoren können nicht exportiert werden.

Aufgaben importieren

Sie können Gruppenaufgaben und Aufgaben für bestimmte Geräte importieren. Die Aufgaben des Administrationsservers und die lokalen Aufgaben sind für den Import nicht verfügbar.

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

1. Wählen Sie die Aufgabenliste, in welche die Aufgabe importiert werden soll:
   - Wenn Sie die Aufgabe in die Liste mit Gruppenaufgaben importieren möchten, wählen Sie im Arbeitsplatz der gewählten Administrationsgruppe die Registerkarte **Aufgaben** aus.
   - Wenn Sie die Aufgabe in die Liste mit Aufgaben für bestimmte Geräte importieren möchten, wählen Sie in der Konsolenstruktur den Ordner **Aufgaben für bestimmte Geräte** aus.
2. Wählen Sie eine der folgenden Methoden für den Import der Aufgabe aus:
   - Klicken Sie mit der rechten Maustaste auf die Aufgabenliste und wählen **Alle Aufgaben** → **Importieren** aus.
   - Klicken Sie im Block zur Verwaltung der Aufgabenliste auf den Link **Aufgabe aus Datei importieren**.
3. Geben Sie im folgenden Fenster den Pfad zur Datei an, aus der Sie die Aufgabe importieren wollen.
4. Klicken Sie auf **Öffnen**.

Daraufhin wird die importierte Aufgabe in der Aufgabenliste angezeigt.

Wenn in der gewählten Liste eine Aufgabe mit dem gleichen Namen wie die zu importierende Aufgabe bereits vorhanden ist, wird dem Namen der zu importierenden Aufgabe eine Endung der Form **(<laufende Nummer>)** angehängt. Beispiel: **(1)**, **(2)**.

Aufgaben konvertieren

Kaspersky Security Center ermöglicht es, die Aufgaben vorheriger Versionen der Kaspersky-Lab-Programme in die Aufgaben aktueller Programmversionen zu konvertieren.

Die Konvertierung von Aufgaben ist für die folgenden Programme möglich:

- Kaspersky Anti-Virus 6.0 für Windows Workstation MP4
- Kaspersky Endpoint Security 8 für Windows
- Kaspersky Endpoint Security 10 für Windows.

Um Aufgaben konvertieren zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus, für den Aufgaben konvertiert werden sollen.
2. Wählen Sie im Kontextmenü des Administrationsservers den Punkt **Alle Aufgaben** → **Assistent für die Stapelkonvertierung von Richtlinien und Aufgaben**.

   Daraufhin wird der Assistent zum Konvertieren von Richtlinien und Aufgaben gestartet. Folgen Sie den Anweisungen.

Nach Fertigstellung des Assistenten werden neue Aufgaben erstellt, die die Einstellungen vorheriger Programmversionen verwenden.

Aufgaben manuell starten und beenden

Sie können die Aufgaben auf zwei Arten starten und beenden: mithilfe des Kontextmenüs der Aufgabe und im Eigenschaftenfenster des Client-Geräts, für das diese Aufgabe bestimmt wurde.

> Gruppenaufgaben können von Benutzern, die der Gruppe **KLAdmins (s. Abschnitt "Zugriffsberechtigungen für den Administrationsserver und dessen Objekte" auf S.** 97**)** angehören, aus dem Kontextmenü des Geräts gestartet werden.

Gehen Sie wie folgt vor, um eine Aufgabe vom Kontextmenü oder vom Eigenschaftenfenster der Aufgabe aus zu starten bzw. zu beenden:

1. Wählen Sie in der Aufgabenliste die Aufgabe aus.

2. Starten Sie oder beenden die Aufgabe auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen **Starten** oder **Stop** aus.

   - Klicken Sie im Abschnitt **Allgemein** im Eigenschaftenfenster der Aufgabe auf **Starten** oder **Stop**.

Gehen Sie wie folgt vor, um eine Aufgabe vom Kontextmenü oder vom Eigenschaftenfenster des Client-Geräts aus zu starten bzw. zu beenden:

1. In der Liste der Geräte wählen Sie das Gerät aus.

2. Starten Sie oder beenden die Aufgabe auf eine der folgenden Weisen:

   - Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben** → **Aufgabe starten**. Wählen Sie in der Liste die gewünschte Aufgabe.

     Die Liste der Geräte, für welche die Aufgabe bestimmt wurde, wird durch das gewählte Gerät ersetzt. Die Aufgabe wird gestartet.

   - Klicken Sie im Eigenschaftenfenster des Geräts im Abschnitt **Aufgaben** auf die Schaltfläche  oder  .

Aufgaben manuell fortsetzen und anhalten

Um die Ausführung einer Aufgabe anzuhalten oder fortzusetzen, gehen Sie wie folgt vor:

1. Wählen Sie in der Aufgabenliste die Aufgabe aus.
2. Halten Sie die Aufgabe an oder setzen Sie die Ausführung der Aufgabe auf eine der folgenden Weisen fort:
   - Klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Anhalten** oder **Fortsetzen** aus.
   - Klicken Sie im Abschnitt **Allgemein** im Eigenschaftenfenster der Aufgabe auf **Anhalten** oder **Fortsetzen**.

Aufgabenausführung überwachen

Um die Aufgabenausführung zu überwachen, gehen Sie wie folgt vor:

Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.

Im mittleren Fensterbereich des Abschnitts **Allgemein** werden Informationen über den aktuellen Status der Aufgabe angezeigt.

Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen

Kaspersky Security Center ermöglicht die Anzeige von Ausführungsergebnissen der Gruppenaufgaben, Aufgaben für bestimmte Geräte und Aufgaben des Administrationsservers. Die Ausführungsergebnisse der lokalen Aufgaben können nicht angezeigt werden.

Um sich die Ergebnisse der Aufgabenausführung anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.

Filter für die Informationen über die Ergebnisse der Aufgabenausführung konfigurieren

Kaspersky Security Center ermöglicht das Filtern von Informationen über die Ausführungsergebnisse der Gruppenaufgaben, Aufgaben für bestimmte Geräte und Aufgaben des Administrationsservers. Für die lokalen Aufgaben ist der Filter nicht verfügbar.

Um den Filter für die Informationen über die Ergebnisse der Aufgabenausführung einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.

2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.

   In der Tabelle im oberen Bereich des Fensters wird die Liste aller Geräte angezeigt, für die die Aufgabe zugewiesen wurde. In der Tabelle im unteren Bereich des Fensters werden die Ergebnisse der Aufgabenausführung des ausgewählten Geräts angezeigt:

3. Öffnen Sie in der gewünschten Tabelle mithilfe der rechten Maustaste das Kontextmenü und wählen Sie darin den Punkt **Filter**.

4. Konfigurieren Sie im folgenden Fenster **Filter anwenden** in den Abschnitten **Ereignisse**, **Geräte** und **Uhrzeit** die Einstellungen für den Filter. Klicken Sie auf die Schaltfläche **OK**.

Im Fenster **Ergebnisse der Aufgabenausführung** werden jetzt die Informationen angezeigt, die den eingegebenen Filtereinstellungen entsprechen.

Ändern der Aufgabe Rollback der Änderungen

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

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

2. Wählen Sie im Arbeitsplatz des Ordners **Aufgaben** die Aufgabe aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Aufgabe.

3. Nehmen Sie die notwendigen Änderungen vor.

   > Im Abschnitt **Ausnahmen vom Aufgabengültigkeitsbereich** kann die Liste der Untergruppen, auf die sich die Aufgabe nicht erstrecken soll, angepasst werden.

4. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die Änderungen der Aufgabe werden in den Eigenschaften der Aufgabe, im Abschnitt **Revisionsverlauf** gespeichert.

Notfalls können Sie die Änderungen der Aufgabe zurücksetzen.

Um die Änderungen einer Aufgabe zurückzusetzen, gehen Sie wie folgt vor:

1. Wahlen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Wählen Sie die Aufgabe, deren Änderungen zurückgesetzt werden sollen, aus und wechseln Sie mithilfe des Kontextmenüs zum Eigenschaftenfenster der Aufgabe.
3. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Revisionsverlauf** aus.
4. Wählen Sie in der Liste mit den Aufgabenrevisionen die Nummer der Revision aus, deren Änderungen zurückgesetzt werden sollen.
5. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Rollback**.

Lokale Einstellungen des Programms anzeigen und ändern

Die Verwaltung durch Kaspersky Security Center ermöglicht, lokale Programmeinstellungen auf den Geräten über die Verwaltungskonsole im Remote-Betrieb zu verwalten.

Bei lokalen Programmeinstellungen handelt es sich um die Programmeinstellungen, die für ein Gerät individuell sind. Mit Kaspersky Security Center können Sie lokale Programmeinstellungen für Geräte bestimmen, die zu Administrationsgruppen gehören.

Einstellungen für Kaspersky-Lab-Programme sind in den Handbüchern der jeweiligen Programme ausführlich beschrieben.

Um die lokalen Einstellungen eines Programms anzuzeigen oder zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Arbeitsplatz der Gruppe, zu welcher das gewünschte Gerät gehört, auf die Registerkarte **Geräte**.

2. Im Eigenschaftenfenster des Geräts im Abschnitt **Programme** wählen Sie das gewünschte Programm aus.

3. Öffnen Sie durch Doppelklick auf den Namen des Programms oder durch Klicken auf die Schaltfläche **Eigenschaften** das Programmeigenschaftenfenster.

Daraufhin wird das Fenster mit den lokalen Einstellungen des gewählten Programms geöffnet, die Sie sich anzeigen lassen und geändert werden können.

Sie können die Einstellungen ändern, deren Änderung durch die Gruppenrichtlinie nicht verboten wird (Einstellungen, die in der Richtlinie mit einem "Schloss" nicht verriegelt sind).

Client-Geräte verwalten

Der Abschnitt enthält Informationen über die Arbeit mit den Client-Geräten.

In diesem Abschnitt

Client-Geräte mit dem Administrationsserver verbinden

Eine Verbindung zwischen einem Client-Gerät und dem Administrationsserver wird durch den auf dem Client-Gerät installierten Administrationsagenten hergestellt.

Beim Herstellen einer Verbindung zwischen dem Client-Gerät und dem Administrationsserver werden folgende Vorgänge ausgeführt:

- Automatische Synchronisierung der Daten:
  - Synchronisierung der Liste der Programme, die auf dem Client-Gerät installiert sind
  - Synchronisierung von Richtlinien, Programmeinstellungen, Aufgaben und Aufgabeneinstellungen
- Empfang von aktuellen Daten über den Status der Programme, Aufgabenausführung und Statistikdaten der Programme durch den Administrationsserver
- Senden der Daten an den Administrationsserver über die Ereignisse, die verarbeitet werden sollen.

Die automatische Datensynchronisierung erfolgt regelmäßig in Abhängigkeit von den Einstellungen des Administrationsagenten (beispielsweise alle 15 Minuten). Sie können das Intervall zwischen den Verbindungsaufbauten manuell angeben.

Die Ereignisdaten werden sofort nach Eintritt des Ereignisses an den Administrationsserver gesendet.

Kaspersky Security Center ermöglicht es, die Verbindung zwischen einem Client-Gerät und dem Administrationsserver so einzustellen, dass die Verbindung nach Abschluss eines Vorgangs nicht getrennt wird. Eine ununterbrochene Verbindung wird dann gebraucht, wenn der Programmstatus ständig kontrolliert werden soll und der Administrationsserver keine Verbindung zum Client-Gerät herstellen kann (Die Verbindung ist beispielsweise durch eine Firewall geschützt, Ports dürfen auf dem Client-Gerät nicht geöffnet werden, IP-Adresse des Client-Geräts ist nicht bekannt usw.). Eine ununterbrochene Verbindung zwischen einem Client-Gerät und dem Administrationsserver können Sie im Eigenschaftenfenster des Client-Geräts im Abschnitt **Allgemein** herstellen.

Es wird empfohlen, mit den wichtigsten Geräten eine ununterbrochene Verbindung herzustellen. Die Gesamtzahl der vom Administrationsserver gleichzeitig unterstützten Verbindungen ist beschränkt (einige hundert).

Bei einer manuellen Synchronisierung wird eine Hilfsmethode für das Herstellen einer Verbindung verwendet. Bei dieser Methode wird die Verbindung durch den Administrationsserver initiiert. Öffnen Sie vor dem Verbindungsaufbau den entsprechenden UDP-Port auf dem Client-Gerät. Der Administrationsserver schickt die Anfrage zum Verbindungsaufbau an den UDP-Port des Client-Geräts. Daraufhin wird das Zertifikat des Administrationsserver überprüft. Stimmt das Zertifikat des Servers mit dessen Kopie auf dem Client-Gerät überein, wird die Verbindung aufgebaut.

Der manuelle Start des Synchronisierungsvorgangs wird verwendet, wenn Sie aktuelle Informationen über den Status der Programme, Aufgabenausführung und Statistikdaten über die Programme empfangen möchten.

Client-Gerät manuell mit Administrationsserver verbinden. Tool klmover

Wenn es erforderlich ist, ein Client-Gerät mit dem Administrationsserver manuell zu verbinden, können Sie das Tool klmover auf dem Client-Gerät verwenden.

Bei der Installation des Administrationsagenten auf dem Client-Gerät wird das Tool automatisch in den Installationsordner des Administrationsagenten kopiert.

Um ein Client-Gerät zum Administrationsserver mit dem Tool klmover manuell zu verbinden,

starten Sie auf dem Gerät das Tool klmover über die Befehlszeile.

Beim Starten über die Befehlszeile führt es je nach Parameter die folgenden Aktionen aus:

- Verbinden des Administrationsagenten mit dem Administrationsserver mit den angegebenen Einstellungen
- Eintragen der Ergebnisse dieses Vorgangs in die Log-Datei oder Darstellung der Ergebnisse auf dem Bildschirm.

Die Syntax des Tools lautet:

```
klmover [-logfile <Dateiname>] [-address <Serveradresse>] [-pn
<Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad
zur Zertifikatsdatei>] [-silent] [-dupfix]
```

Die Schlüssel weisen folgende Bedeutung auf:

- `-logfile <Dateiname>` – Ergebnisse der Tool-Ausführung in Log-Datei schreiben.

  Standardmäßig werden die Informationen im Standardausgabe-Stream (stdout) gespeichert. Wenn der Schlüssel nicht verwendet wird, werden die Ergebnisse und Fehlermeldungen auf dem Bildschirm angezeigt.

- `-address <Serveradresse>` – Adresse des Administrationsservers, zu dem eine Verbindung hergestellt werden soll.

  Es kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name des Geräts angegeben werden.

- `-pn <Portnummer>` – Nummer des Ports, über den eine ungesicherte Verbindung zum Administrationsserver hergestellt wird.

  Standardmäßig wird Port 14000 verwendet.

- `-ps <SSL-Portnummer>` – Nummer des SSL-Ports, über den eine gesicherte Verbindung zum Administrationsserver mit dem SSL-Protokoll hergestellt wird.

  Standardmäßig wird Port 13000 verwendet.

- `-nossl` – Ungesicherte Verbindung zum Administrationsserver verwenden.

  Wenn kein Schlüssel verwendet wird, erfolgt die Verbindung des Administrationsagenten mit dem Administrationsserver über das SSL-Protokoll.

- `-cert <Pfad zur Zertifikatsdatei>` – Angegebene Zertifikatsdatei für Authentifizierung am Administrationsserver verwenden.

  Wenn kein Schlüssel angegeben wird, empfängt der Administrationsagent das Zertifikat beim ersten Verbinden mit dem Administrationsserver.

- `-silent` – Tool im Silent-Modus starten.

  Der Einsatz dieses Parameters kann sehr nützlich sein, wenn das Tool beispielsweise über ein Anmeldeskript bei der Anmeldung eines Benutzers aufgerufen wird.

- `-dupfix` – Dieser Schlüssel kommt zum Einsatz, wenn der Administrationsagent nicht auf die konventionelle Weise mit den Dateien im Lieferumfang, sondern beispielsweise über die Wiederherstellung eines Disk-Images installiert wurde.

Verbindung des Client-Geräts mit dem Administrationsserver tunneln

Es ist erforderlich, die Verbindung eines Remote-Geräts mit dem Administrationsserver zu tunneln, wenn der Port für die Verbindung mit dem Administrationsserver auf dem Gerät nicht verfügbar ist. Der Port auf dem Gerät kann in folgenden Fällen nicht verfügbar sein:

- Das Remote-Gerät ist mit dem lokalen Netzwerk verbunden, in dem das NAT-Verfahren verwendet wird.

- Das Remote-Gerät gehört zum lokalen Netzwerk des Administrationsservers, sein Port wird jedoch von der Firewall geschlossen.

Um die Verbindung zwischen einem Client-Gerät und dem Administrationsserver zu tunneln, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner der Gruppe, zu welcher das Client-Gerät gehört.

2. Wählen Sie auf der Registerkarte **Geräte** ein Gerät aus.

3. Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben** → **Verbindung tunneln**.

4. Erstellen Sie im folgenden Fenster **Verbindung tunneln** einen Tunnel.

Remotedesktopverbindung mit dem Client-Gerät herstellen

Der Administrator kann Remotezugriff auf den Desktop des Client-Geräts mithilfe des Administrationsagenten bekommen, der auf dem Client-Gerät installiert wurde. Die Remoteverbindung mit dem Client-Gerät mithilfe des Administrationsagenten ist auch dann möglich, wenn die TCP- und UDP-Ports des Client-Geräts für den Zugriff gesperrt sind.

Nach der Verbindung mit dem Gerät bekommt der Administrator vollständigen Zugriff auf die Informationen dieses Geräts und kann die auf diesem Gerät installierten Programme verwalten.

Die Remoteverbindung mit dem Client-Gerät kann auf zwei Arten hergestellt werden:

- Mithilfe der Standard-Komponente von Microsoft Windows "Remotedesktopverbindung". Die Remotedesktopverbindung erfolgt mithilfe des Windows-Standardtools mstsc.exe gemäß den Einstellungen des Tools.

  Die Verbindung zu einer bestehenden Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Nachdem sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne vorherige Benachrichtigung von der Sitzung abgemeldet.

- Mithilfe der Windows-Technologie Desktopfreigabe. Bei der Verbindung mit einer vorhandenen Remotedesktop-Sitzung empfängt der Benutzer der Sitzung auf dem Gerät eine Anfrage zum Herstellen der Verbindung vom Administrator. Die Informationen über die Aktivitäten auf dem Remote-Gerät und deren Ergebnisse werden in den Kaspersky Security Center-Berichten nicht gespeichert.

  Der Administrator kann eine Verbindung mit der vorhandenen Sitzung auf dem Client-Gerät herstellen, ohne dass der Benutzer dieser Sitzung getrennt wird. In diesem Fall haben

der Administrator und der Benutzer der Sitzung auf dem Gerät einen gemeinsamen Zugriff auf den Desktop.

Der Administrator kann ein Audit der Aktionen auf dem Remote-Client-Gerät konfigurieren. Während des Audits werden Informationen über die Dateien auf dem Client-Gerät gesammelt, die vom Administrator geöffnet bzw. geändert werden (s. Abschnitt "Audit der Aktionen auf einem Remote-Client-Gerät" auf S. 158).

Zum Herstellen einer Remotedesktopverbindung mit dem Client-Gerät mithilfe der Windows-Technologie Desktopfreigabe müssen die folgenden Anforderungen erfüllt werden:

- Auf dem Client-Gerät ist das Betriebssystem Microsoft Windows Vista oder eine höhere Version installiert.
- Im Administrator-Arbeitsplatz ist das Betriebssystem Microsoft Windows Vista oder eine höhere Version installiert. Für die Herstellung einer Verbindung mithilfe der Windows-Technologie Desktopfreigabe gibt es keine Einschränkungen hinsichtlich des Betriebssystemtyps des Geräts, auf dem der Administrationsserver installiert ist.
- Kaspersky Security Center nutzt eine Lizenz für Systems Management.

Gehen Sie wie folgt vor, um eine Remotedesktopverbindung mit dem Client-Gerät mithilfe der Komponente "Remotedesktopverbindung" herzustellen:

1. Wählen Sie in der Verwaltungskonsole ein Client-Gerät aus, auf das zugegriffen werden soll.
2. Wählen Sie im Kontextmenü des Client-Geräts den Punkt **Alle Aufgaben** → **Mit Gerät verbinden** → **Neue RDP-Sitzung erstellen**.

   Daraufhin wird das Windows-Standardtool mstsc.exe zum Herstellen einer Remotedesktopverbindung gestartet.
3. Folgen Sie den Anweisungen in den Fenstern des Tools.

Nach der Verbindung mit dem Client-Gerät ist der Desktop des Client-Geräts im Microsoft Windows-Fenster zur Remoteverbindung verfügbar.

Um eine Verbindung mit dem Client-Gerät-Desktop über Windows Desktopfreigabe herzustellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsole ein Client-Gerät aus, auf das zugegriffen werden soll.

2. Wählen Sie im Kontextmenü des Geräts den Punkt **Alle Aufgaben** → **Mit Gerät verbinden** → Gemeinsamer Zugriff auf den Arbeitsplatz.

3. Wählen Sie im folgenden Fenster **Desktopsitzung auswählen** die Sitzung auf dem Client-Gerät, zu der eine Verbindung hergestellt werden soll.

   Bei einer erfolgreichen Verbindung mit dem Client-Gerät wird sein Desktop im Fenster **Kaspersky Remote desktop session viewer** verfügbar.

4. Zur Interaktion mit dem Gerät wählen Sie im Hauptmenü des Fensters **Kaspersky Remote desktop session viewer** die Option **Aktionen** → **Interaktivmodus**.

Siehe auch:

Lizenzierungsvarianten für Kaspersky Security Center 67

Einstellungen für den Neustart des Client-Geräts

Während der Ausführung, Installation oder Deinstallation von Kaspersky Security Center kann es erforderlich sein, dass ein Neustart des Client-Geräts durchgeführt wird. Die Einstellungen für den Neustart des Geräts können im Programm angepasst werden.

Um die Einstellungen für den Neustart des Client-Geräts anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für welche der Neustart angepasst werden soll.

2. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien** aus.

3. Wählen Sie die Richtlinie des Administrationsagenten von Kaspersky Security Center aus der Richtlinienliste aus, und wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften**.

4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Verwaltung des Neustarts**.

5. Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn ein Neustart des Geräts erforderlich ist.

   - Wählen Sie die Option **Betriebssystem nicht neu starten**, wenn Sie einen automatischen Neustart unterbinden möchten.
   - Wählen Sie **Bei Bedarf das Betriebssystem automatisch neu starten**, wenn Sie einen automatischen Neustart erlauben möchten.
   - Wählen Sie **Benutzer fragen**, wenn Sie die Zustimmung des Benutzers zum Neustart aktivieren möchten.

   Sie können die Häufigkeit der Abfrage eines Neustarts angeben, einen erzwungenen Neustart und ein erzwungenes Schließen des Programms in gesperrten Sitzungen auf dem Gerät aktivieren, indem Sie die entsprechenden Kontrollkästchen aktivieren.

6. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Eigenschaftenfenster der Richtlinie zu schließen.

Als Ergebnis des Neustarts wird das Betriebssystem auf dem Gerät konfiguriert.

Überwachung der Aktionen auf einem Remote-Client-Gerät

Das Programm ermöglicht die Durchführung eines Audits der Aktionen des Administrators auf einem Remote-Client-Gerät. Während des Audits werden Informationen über die Dateien auf dem Gerät gesammelt, die vom Administrator geöffnet bzw. geändert werden. Das Audit des Administrators ist unter folgenden Bedingungen verfügbar:

- Es ist eine gültige Lizenz für Systems Management vorhanden.
- Der Administrator verfügt über die Berechtigung zum Start der Desktopfreigabe auf dem Remote-Gerät.

Um das Audit auf dem Remote-Gerät zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe aus, für die das Audit der Aktionen des Administrators konfiguriert werden soll.
2. Wählen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien** aus.
3. Wählen Sie die Richtlinie des Administrationsagenten von Kaspersky Security Center, und wählen Sie im Kontextmenü der Richtlinie den Punkt **Eigenschaften**.
4. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Desktopfreigabe**.
5. Aktivieren Sie das Kontrollkästchen **Audit aktivieren**.
6. Fügen Sie in den Listen **Masken für Dateien, für die das Lesen geloggt werden soll** und **Masken für Dateien, für die Änderungen geloggt werden sollen** die Dateimasken hinzu, für die Aktionen während des Audits geloggt werden sollen.

   Standardmäßig werden Aktionen mit Dateien mit den Erweiterungen txt, rtf, doc, xls, docx, xlsx, odt, pdf geloggt.
7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern und das Eigenschaftenfenster der Richtlinie zu schließen.

Als Ergebnis wird das Audit der Aktionen des Administrators auf dem Remote-Gerät des Benutzers bei Verwendung der Desktopfreigabe konfiguriert.

Einträge über die Aktionen des Administrators auf dem Remote-Gerät werden wie folgt gespeichert:

- Im Ereignisprotokoll auf dem Remote-Gerät
- In einer Datei mit der Erweiterung syslog, die sich im Ordner des Administrationsagenten auf dem Remote-Gerät befindet (beispielsweise C:\Programme\KasperskyLab\adminkit\1103\logs)
- In der Ereignisdatenbank von Kaspersky Security Center.

Verbindung des Client-Geräts mit dem Administrationsserver prüfen

Kaspersky Security Center ermöglicht es, Verbindungen zwischen einem Client-Gerät und dem Administrationsserver automatisch oder manuell zu überprüfen.

Die automatische Überprüfung der Verbindung erfolgt auf dem Administrationsserver. Die manuelle Überprüfung der Verbindung erfolgt auf dem Gerät.

In diesem Abschnitt

Verbindung des Client-Geräts mit dem Administrationsserver automatisch prüfen

Um die automatische Überprüfung der Verbindung zwischen einem Client-Gerät und dem Administrationsserver auszuführen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die entsprechende Administrationsgruppe des Geräts aus.

2. Wählen Sie im Arbeitsplatz der Administrationsgruppe auf der Registerkarte **Geräte** das gewünschte Gerät aus.

3. Wählen Sie im Kontextmenü des Geräts den Punkt **Verfügbarkeit des Geräts prüfen**.

Im folgenden Fenster werden Daten über die Verfügbarkeit des Geräts angezeigt.

Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk

Sie können die Verbindung zwischen einem Client-Gerät und dem Administrationsserver mit dem Tool klnagchk überprüfen. Darüber hinaus können Sie mit dem Tool ausführliche Informationen über die Verbindungseinstellungen zwischen dem Client-Gerät und dem Administrationsserver erhalten.

Bei der Installation des Administrationsagenten auf dem Gerät wird das Tool automatisch in den Installationsordner des Administrationsagenten kopiert.

Beim Starten über die Befehlszeile führt es je nach Parameter die folgenden Aktionen aus:

- Zeigt eine Meldung auf dem Bildschirm an oder nimmt eine Eintragung in der Log-Datei der Einstellungswerte für die Verbindung vor, die zwischen dem Administrationsagenten des Geräts und dem Administrationsserver besteht.

- Eintragung in die Log-Datei einer Statistik für den Administrationsagenten vornehmen (beginnend mit dem letzten Start dieser Komponente) und die Ausführungsergebnisse für das Tool oder die Meldung auf dem Bildschirm anzeigen.

- Den Versuch unternehmen, eine Verbindung zwischen dem Administrationsagenten und Administrationsserver herzustellen.

  Bei fehlgeschlagenem Verbindungsaufbau sendet das Tool ein ICMP-Paket an das Gerät, um den Status des Geräts zu überprüfen, auf dem der Administrationsserver installiert ist.

Um die Verbindung zwischen einem Client-Gerät und dem Administrationsserver mit dem Tool klnagchk zu überprüfen,

starten Sie auf dem Gerät das Tool klnagchk über die Befehlszeile.

Die Syntax des Tools lautet:

```
klnagchk [-logfile <Dateiname>] [-sp] [-savecert <Pfad
zur Zertifikatsdatei>] [-restart]
```

Die Schlüssel weisen folgende Bedeutung auf:

- `-logfile <Dateiname>` – Parameterwerte für Verbindung zwischen Administrationsagenten und Server sowie die Ergebnisse der Ausführung des Tools in die Log-Datei schreiben.

  Standardmäßig werden die Informationen im Standardausgabe-Stream (stdout) gespeichert. Wenn der Schlüssel nicht verwendet wird, werden die Einstellungen, Ergebnisse und Fehlermeldungen auf dem Bildschirm angezeigt.

- `-sp` – Kennwortabfrage für Authentifizierung des Benutzers am Proxy-Server.

  Die Einstellung wird eingesetzt, wenn die Verbindung zum Administrationsserver über einen Proxy-Server aufgebaut wird.

- `-savecert <Dateiname>` – Zertifikat zur Authentifizierung des Zugangs am Administrationsserver in der angegebenen Datei speichern.

- `-restart` – Administrationsagent nach Abschluss des Tools neu starten.

Client-Geräte auf dem Administrationsserver identifizieren

Die Client-Geräte werden anhand ihrer Namen identifiziert. Der Name des Geräts ist einzigartig unter allen Namen der Geräte, die mit dem Administrationsserver verbunden sind.

Der Name des Geräts wird beim Durchsuchen des Windows-Netzwerks und beim Erkennen eines neuen Geräts oder beim ersten Verbindungsaufbau des auf dem Gerät installierten Administrationsagenten zum Administrationsserver an den Server weitergegeben. Standardmäßig stimmt der Name mit dem Namen des Geräts im Windows-Netzwerk (NetBIOS-Name) überein. Wenn auf dem Administrationsserver ein Gerät mit dem gleichen Namen bereits registriert ist, wird dem neuen Gerät eine Endung mit einer Ordnungszahl wie **<Name>-1**, **<Name>-2** hinzugefügt. Unter diesem Namen wird das Gerät in die Administrationsgruppe übernommen.

Geräte zu Administrationsgruppe hinzufügen

Um eines oder mehrere Geräte zu einer gewählten Administrationsgruppe hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte**.

2. Wählen Sie im Ordner **Verwaltete Geräte** den Unterordner aus, der der Gruppe entspricht, in die Client-Geräte aufgenommen werden sollen.

   Wenn Geräte zur Gruppe **Verwaltete Geräte** hinzugefügt werden sollen, können Sie diesen Schritt überspringen.

3. Um Geräte zu einer Gruppe hinzuzufügen, gehen Sie im Arbeitsplatz der gewählten Administrationsgruppe auf der Registerkarte **Geräte** wie folgt vor:

   - Klicken Sie im Block zur Verwaltung der Geräteliste auf den Link **Geräte hinzufügen**.
   - Klicken Sie mit der rechten Maustaste auf die Liste der Geräte und wählen **Erstellen** → **Gerät** aus.

   Daraufhin wird der Assistent für das Hinzufügen von Geräten gestartet. Folgen Sie den Anweisungen. Legen Sie dabei fest, wie die Geräte zur Gruppe hinzugefügt werden sollen, und erstellen Sie eine Liste der Geräte, die zu der Gruppe gehören.

   Wenn Sie die Geräteliste manuell erstellen, können Sie als Gerätadresse die IP-Adresse (bzw. das IP-Intervall), den NetBIOS- bzw. DNS-Namen verwenden. Manuell können zur Geräteliste nur die Geräte hinzugefügt werden, deren Informationen bei der Verbindung mit dem Gerät oder nach einer Netzwerkabfrage in die Datenbank des Administrationsservers bereits eingetragen wurden.

   Um die Geräteliste aus einer Datei zu importieren, geben sie die TXT-Datei mit dem Verzeichnis der Adressen für Geräte, die hinzugefügt werden sollen. Dabei muss jede Adresse in einer separaten Zeile aufgeführt sein.

Nach Abschluss des Assistenten werden die gewählten Geräte in die Administrationsgruppe aufgenommen und in der Geräteliste mit den Namen angezeigt, die der Administrationsserver bestimmt hat.

> Sie können ein Gerät auch zur gewählten Administrationsgruppe hinzufügen, indem Sie den Computer mit der Maus aus dem Ordner **Nicht zugeordnete Geräte** in den Ordner der Administrationsgruppe verschieben.

Administrationsserver für Client-Geräte wechseln

Sie können den Administrationsserver, der die Client-Geräte verwaltet, durch einen anderen Administrationsserver mit der Aufgabe **Administrationsserver wechseln** ersetzen.

Um einen Administrationsserver, der die Client-Geräte verwaltet, zu wechseln, gehen Sie wie folgt vor:

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

2. Erstellen Sie eine Aufgabe zum Wechsel des Administrationsservers auf eine der folgenden Weisen:

   - Um den Administrationsserver für Geräte zu wechseln, die zur gewählten Administrationsgruppe gehören, erstellen Sie eine Aufgabe für die gewählte Gruppe (s. Abschnitt "Gruppenaufgaben erstellen" auf S. 136).

   - Um den Administrationsserver für Geräte zu wechseln, die zu verschiedenen Administrationsgruppen oder zu keiner Administrationsgruppe gehören, erstellen Sie eine Aufgabe für bestimmte Geräte (s. Abschnitt "Aufgaben für bestimmte Geräte erstellen" auf S. 138).

   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 den Knoten **Kaspersky Security Center** aus, öffnen Sie den Ordner **Erweitert** und wählen Sie die Aufgabe **Administrationsserver wechseln** aus.

3. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe werden die Client-Geräte, für welche die Aufgabe erstellt wurde, auf den Administrationsserver umgestellt, der in den Einstellungen der Aufgabe angegeben wurde.

Wenn der Administrationsserver die Funktionen Verschlüsselung und Datenschutz unterstützt, wird beim Erstellen der Aufgabe **Administrationsserver wechseln** eine Warnung angezeigt, dass bei Vorhandensein von verschlüsselten Daten, bei der Umstellung der Geräte auf einen anderen Server, nur die verschlüsselten Daten freigegeben werden, mit denen die Benutzer bereits gearbeitet haben. In anderen Fällen werden die Daten nicht freigegeben. Eine ausführliche Beschreibung der Fälle, in denen die verschlüsselten Daten nicht freigegeben werden, können Sie dem Administratorhandbuch für Kaspersky Endpoint Security 10 für Windows entnehmen.

Client-Geräte von einem entfernten Standort einschalten, ausschalten und Neustart durchführen

Kaspersky Security Center ermöglicht die Remoteverwaltung (Einschalten, Ausschalten und Neustarten) von Client-Geräten.

Um Client-Geräte im Remote-Betrieb zu verwalten, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die Geräte verwaltet.
2. Erstellen Sie eine Aufgabe zur Verwaltung eines Geräts auf eine der folgenden Weisen:
   - Um Geräte aus der gewählten Administrationsgruppe einzuschalten, auszuschalten oder neu zu starten, erstellen Sie eine Aufgabe für die gewählte Gruppe (s. Abschnitt "Gruppenaufgaben erstellen" auf S. 136).
   - Um Geräte aus verschiedenen Administrationsgruppen oder Geräte, die zu keiner Administrationsgruppe gehören, einzuschalten, auszuschalten oder neu zu starten, erstellen Sie eine Aufgabe für bestimmte Geräte (s. Abschnitt "Aufgaben für bestimmte Geräte erstellen" auf S. 138).

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 den Knoten **Kaspersky Security Center** aus, öffnen Sie den Ordner **Erweitert** und wählen Sie die Aufgabe **Verwaltung der Geräte** aus.

3. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe wird der Befehl (Einschalten, Ausschalten oder Neustarten) auf ausgewählten Geräten ausgeführt.

Nachricht an Gerätenutzer senden

Um eine Nachricht an Gerätenutzer zu senden, gehen Sie wie folgt vor:

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

2. Erstellen Sie eine Aufgabe für das Senden einer Nachricht an Gerätenutzer auf eine der folgenden Weisen:

   - Um eine Nachricht an die Benutzer der Geräte zu senden, die zur gewählten Administrationsgruppe gehören, erstellen Sie eine Aufgabe für die gewählte Gruppe (s. Abschnitt "Gruppenaufgaben erstellen" auf S. 136).

   - Um eine Nachricht an die Benutzer der Geräte zu senden, die zu verschiedenen Administrationsgruppen oder zu keiner Administrationsgruppe gehören, erstellen Sie eine Aufgabe für bestimmte Geräte (s. Abschnitt "Aufgaben für bestimmte Geräte erstellen" auf S. 138).

   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 den Knoten **Kaspersky Security Center** aus, öffnen Sie den Ordner **Erweitert** und wählen Sie die Aufgabe **Benutzernachricht** aus.

3. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe wird die Nachricht an die Benutzer der gewählten Geräte gesendet.

Kontrolle über den Status der virtuellen Maschinen

Der Administrationsserver speichert Informationen über den Status der verwalteten Geräte, wie etwa Hardwareinventur und Liste der installierten Programme, Einstellungen der verwalteten Programme, Aufgaben und Richtlinien. Ist ein verwaltetes Gerät eine virtuelle Maschine, dann kann der Benutzer dessen Status aus dem vorher erstellten Abbild der virtuellen Maschine (Snapshot) zu jedem Zeitpunkt wiederherstellen. Daraufhin werden die Informationen über den Status der virtuellen Maschine auf dem Administrationsserver nicht mehr aktuell.

So hat beispielsweise der Administrator eine Schutzrichtlinie um 12:00 auf dem Administrationsserver erstellt, die um 12:01 auf der virtuellen Maschine VM_1 in Kraft trat. Um 12:30 hat der Benutzer der virtuellen Maschine VM_1 den Status der Richtlinie geändert, indem er das um 11:00 erstellte Abbild wiederhergestellt hat. Daraufhin wird die Schutzrichtlinie auf der virtuellen Maschine nicht mehr aktiv. Auf dem Administrationsserver werden jedoch die nicht aktuellen Informationen darüber gespeichert, dass die Schutzrichtlinie auf der virtuellen Maschine VM_1 aktiv ist.

Kaspersky Security Center ermöglicht es, die Änderungen des Status der virtuellen Maschinen zu kontrollieren.

Der Administrationsserver erstellt nach jeder Synchronisierung mit dem Gerät eine eindeutige ID, die sowohl vom Gerät als auch vom Administrationsserver gespeichert wird. Vor dem Beginn der folgenden Synchronisierung vergleicht der Administrationsserver die beiden ID-Werte. Stimmen die ID-Werte nicht überein, betrachtet der Administrationsserver die virtuelle Maschine als eine aus einem Abbild wiederhergestellte. Der Administrationsserver setzt die Richtlinien- bzw. Aufgabeneinstellungen für diese virtuelle Maschine zurück und wendet die aktuellen Richtlinien und Gruppenaufgaben auf sie an.

Geräten automatisch Tags zuweisen

Das Programm kann Geräten automatisch Tags zuweisen. Die automatische Zuweisung von Tags an die Geräte erfolgt mithilfe von Regeln. Diese Regeln zur Zuweisung von Tags können Sie im Eigenschaftenfenster des Administrationsservers und/oder im Eigenschaftenfenster des Geräts erstellen und ändern.

Gehen Sie folgendermaßen vor, um Regeln für die automatische Zuweisung von Tags an Geräte zu erstellen und anzupassen:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Regeln zur Zuweisung von Tags** aus.

4. Klicken Sie im Abschnitt **Regeln zur Zuweisung von Tags** auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird das Fenster **Eigenschaften: Neue Regel** geöffnet.

5. Passen Sie im Abschnitt **Allgemein** des Fensters **Eigenschaften: Neue Regel** die allgemeinen Eigenschaften der Regel an:

   - Geben Sie den Namen der Regel an.

     Der Name der Regel darf nicht mehr als 255 Zeichen umfassen und darf keine Sonderzeiten (*<>-_?:\"|) enthalten.

   - Wählen Sie in der Dropdown-Liste **Tag für die Zuweisung** einen bereits hinzugefügten Tag aus, oder geben Sie einen neuen Tag ein.

   - Aktivieren bzw. deaktivieren Sie die Regel mithilfe des Kontrollkästchens **Regel aktivieren**.

6. Klicken Sie im Abschnitt **Bedingungen** auf die Schaltfläche **Hinzufügen**, um eine neue Bedingung hinzuzufügen, oder klicken Sie auf die Schaltfläche **Eigenschaften**, um eine bestehende Bedingung zu ändern.

   Es wird das Eigenschaftenfenster einer neuen bzw. der bestehenden Bedingung geöffnet.

7. Passen Sie in diesem Fenster die Bedingung für die Zuweisung eines Tags an:

    - Geben Sie im Abschnitt **Allgemein** den Namen der Bedingung an.
    - Konfigurieren Sie im Abschnitt **Netzwerk** die Auslösung der Regel gemäß den Netzwerkeigenschaften des Geräts (Gerätename im Windows-Netzwerk, Zugehörigkeit des Geräts zur Domäne, zum IP-Bereich u. ä.).
    - Konfigurieren Sie im Abschnitt **Active Directory** die Auslösung der Regel anhand der Präsenz des Geräts in einem Unterverzeichnis von Active Directory und gemäß der Mitgliedschaft des Gerätes zur Active Directory Gruppe.
    - Konfigurieren Sie im Abschnitt **Programme** die Auslösung der Regel anhand des Vorhandensein eines Administrationsagenten auf dem Gerät, sowie nach Typ, Version und Architektur des Betriebssystems.
    - Konfigurieren Sie im Abschnitt **Virtuelle Maschinen** die Auslösung der Regel anhand der Zugehörigkeit des Geräts zu verschiedenen Typen von virtuellen Maschinen.
    - Konfigurieren Sie im Abschnitt **Programm-Registry** die Auslösung der Regel anhand des Vorhandenseins von Programmen verschiedenster Hersteller auf dem Gerät.

8. Klicken Sie nach Abschluss der Konfiguration der Bedingung auf die Schaltfläche **OK** im Fenster **Eigenschaften: Neue Bedingung**.

9. Fügen Sie der Regel für die Zuweisung eines Tags weitere Bedingungen hinzu oder konfigurieren Sie diese.

    Die hinzugefügten Auslösungsbedingungen der Regel werden im Eigenschaftenfenster der Regel im Abschnitt **Bedingungen** angezeigt.

10. Klicken Sie im Eigenschaftenfenster der Regel auf die Schaltfläche **OK**.

Die Regel zur Aktivierung des Tags wird gespeichert. Die Regel wird auf Geräten ausgeführt, die den Bedingungen der Regel entsprechen. Nach der Anwendung der Regel wird den Geräten ein Tag zugewiesen. Einem Gerät werden automatisch mehrere Tags zugewiesen, wenn die Regeln für die Zuweisung dieser Tags gleichzeitig ausgeführt werden. Eine Liste aller hinzugefügten Tags können Sie im Eigenschaftenfenster eines beliebigen Geräts im Abschnitt **Tags** anzeigen. Im Abschnitt **Tags** können Sie über den entsprechenden Link auch zur Konfiguration von Regeln für die automatische Zuweisung von Tags wechseln.

Ferndiagnose der Client-Geräte. Kaspersky Security Center Ferndiagnosetool

Das Ferndiagnosetool von Kaspersky Security Center (im Folgenden auch Ferndiagnosetool genannt) dient zur Ausführung folgender Operationen auf den Client-Geräten:

- Ablaufverfolgung aktivieren und deaktivieren, Protokollierungsstufe ändern, Ablaufverfolgungsdatei downloaden
- Anwendungseinstellungen downloaden
- Ereignisprotokolle downloaden
- Diagnose starten und Ergebnisse der Diagnose herunterladen
- Programme starten und beenden.

Das Ferndiagnosetool wird automatisch mit der Verwaltungskonsole auf dem Gerät installiert.

In diesem Abschnitt

Ferndiagnosetool mit dem Client-Gerät verbinden

Um das Ferndiagnosetool mit einem Client-Gerät zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine beliebige Administrationsgruppe aus.

2. Klicken Sie mit der rechten Maustaste im Arbeitsplatz auf der Registerkarte **Geräte** auf das Kontextmenü eines beliebigen Geräts und wählen **Externe Tools** → **Remote-Diagnose** aus.

   Daraufhin wird das Hauptfenster des Ferndiagnosetools geöffnet.

3. Bestimmen Sie im ersten Feld des Hauptfensters, wie das Tool mit dem Gerät verbunden werden soll:

   - **Zugriff mittels Microsoft Windows Netzwerk**
   - **Zugriff mittels Administrationsserver**.

4. Wenn Sie im Hauptfenster des Tools die Option **Zugriff mittels Microsoft Windows Netzwerk** gewählt haben, gehen Sie wie folgt vor:

   - Geben Sie im Feld **Gerät** die Adresse des Geräts an, mit dem das Tool verbunden werden soll.

     Als Geräteadresse kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name angegeben werden.

     In der Standardeinstellung ist die Adresse des Geräts angegeben, aus dessen Kontextmenü das Tool aufgerufen wurde.

   - Geben Sie das Benutzerkonto zur Herstellung der Verbindung mit dem Gerät an:

     - **Im Namen des aktuellen Benutzers verbinden** (Standard): Verbindung unter dem Konto des aktuellen Benutzers herstellen.
     - **Angegebenen Benutzernamen und Kennwort verwenden**: Verbindung unter dem aktuellen Benutzerkonto herstellen. Geben Sie **Benutzername** und **Kennwort** des gewünschten Benutzerkontos an.

Die Verbindung zum Gerät ist nur unter dem Benutzerkonto des lokalen Administrators des Geräts möglich.

5. Bei Auswahl im ersten Feld der Variante **Zugriff mittels Administrationsserver** gehen Sie wie folgt vor:

   - Geben Sie im Feld **Administrationsserver** die Adresse des Administrationsservers an, über den eine Verbindung mit dem Gerät hergestellt werden soll.

     Als Serveradresse kann die IP-Adresse, der NetBIOS-Name oder der DNS-Name angegeben werden.

     In der Standardeinstellung ist die Adresse des Servers angegeben, von dem aus das Tool gestartet wurde.

   - Aktivieren Sie bei Bedarf die Kontrollkästchen **SSL verwenden**, **Daten komprimieren** und **Das Gerät gehört zu untergeordnetem Administrationsserver.**

     Wenn das Kontrollkästchen **Das Gerät gehört zu untergeordnetem Administrationsserver.** aktiviert ist, können Sie im Feld **Untergeordneter Server** einen untergeordneten Administrationsserver auswählen, der das Gerät verwaltet. Klicken Sie dazu auf **Durchsuchen**.

6. Um eine Verbindung mit dem Gerät herzustellen, klicken Sie auf **Einloggen**.

Daraufhin wird das Fenster für Remote-Diagnose des Geräts geöffnet (s. Abb. unten). Im linken Fensterbereich befinden sich die Links für die Ausführung von Vorgängen zur Diagnose des Geräts. Im rechten Fensterbereich wird die Struktur mit den Objekten des Geräts angezeigt, die für das Tool verfügbar sind. Im unteren Fensterbereich wird der Fortschritt der ausgeführten Vorgänge angezeigt.

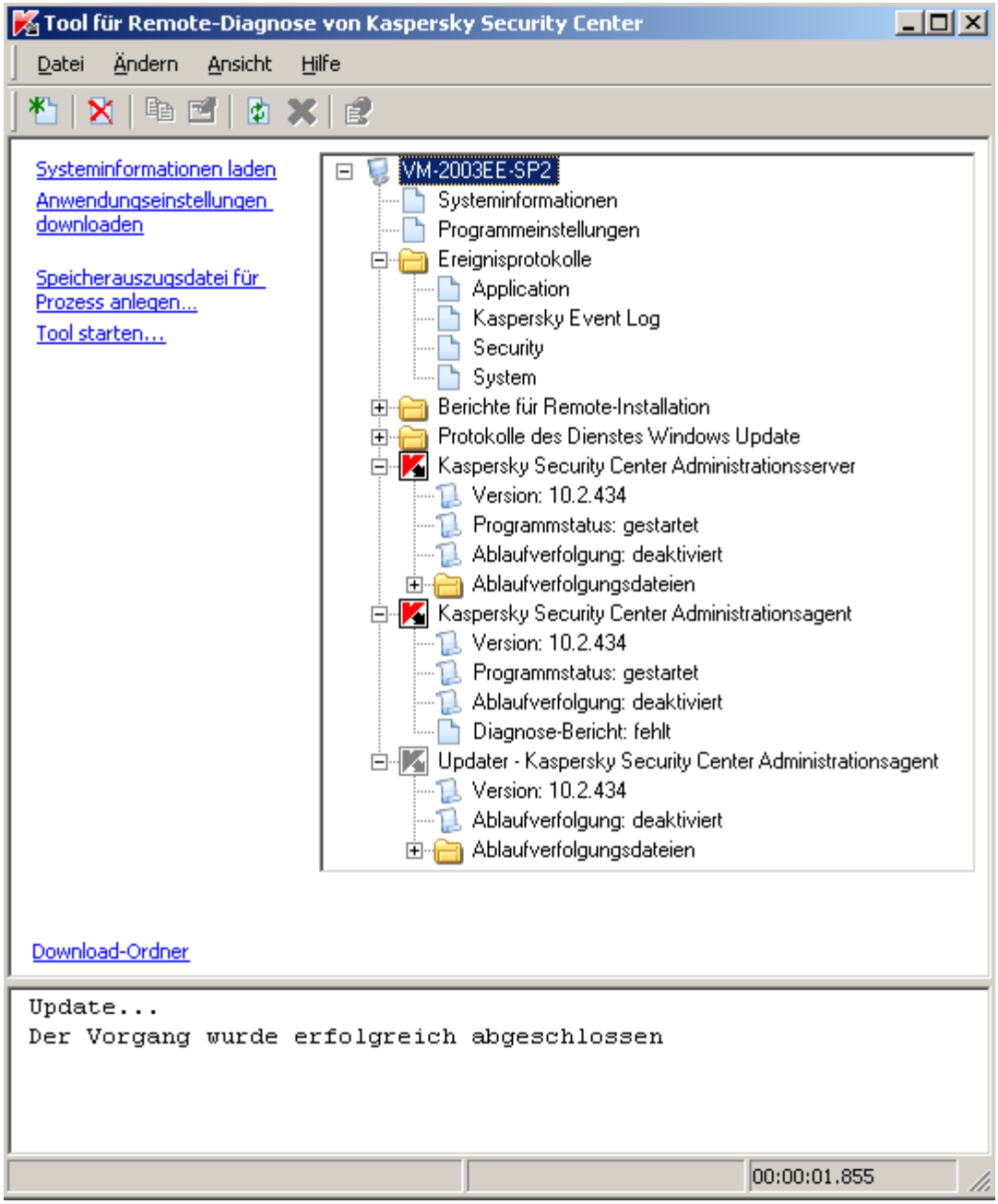


Abbildung 10. Tool zur Remote-Diagnose. Fenster für Remote-Diagnose des Client- Geräts

Das Tool für die Remote-Diagnose speichert die von den Geräten heruntergeladenen Dateien auf dem Desktop des Geräts, von dem aus es gestartet wurde.

Ablaufverfolgung aktivieren und deaktivieren, Protokolldatei downloaden

Um die Protokollierung auf einem Remote-Gerät zu aktivieren, die Protokolldatei herunterzuladen oder die Protokollierung zu deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie das Tool für die Remote-Diagnose, und stellen Sie eine Verbindung mit dem gewünschten Gerät her.

2. Wählen Sie in der Objektstruktur des Geräts das Programm aus, für das die Protokollierung abgerufen werden soll, und klicken Sie im linken Fensterbereich des Tools für Remote-Diagnose auf den Link **Ablaufverfolgung aktivieren**, um die Protokollierung zu aktivieren.

   Die Aktivierung und Deaktivierung der Ablaufverfolgung bei Anwendungen mit Selbstschutz ist nur bei der Verbindung mit dem Gerät mittels Administrationsserver möglich.

   In einigen Fällen ist es erforderlich, das Schutzprogramm und dessen Aufgabe neu zu starten, um die Ablaufverfolgung zu aktivieren.

3. Wählen Sie im Knoten, der dem Programm entspricht, für das die Ablaufverfolgung aktiviert werden soll, im Ordner **Ablaufverfolgungsdateien** die gewünschte Datei aus, und klicken Sie auf den Link **Datei downloaden**, um die Datei herunterzuladen. Bei großen Dateien können nur die letzten Teile der Ablaufverfolgung heruntergeladen werden.

   Sie können die markierte Protokolldatei löschen. Das Löschen der Datei ist jedoch erst nach Deaktivierung der Ablaufverfolgung möglich.

4. Klicken Sie auf den Link **Ablaufverfolgung deaktivieren**, um die Protokollierung zu deaktivieren.

Anwendungseinstellungen downloaden

Um die Programmeinstellungen von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Starten Sie das Tool für die Remote-Diagnose, und stellen Sie eine Verbindung mit dem gewünschten Gerät her.

2. Wählen Sie im Objektbaum im Fenster für Remote-Diagnose des Geräts den oberen Knoten mit dem Namen des Geräts und im linken Fensterbereich die gewünschte Aktion aus:

   - **Systeminformationen laden**

   - **Anwendungseinstellungen downloaden**

   - **Dump-Datei für Prozess anlegen**

     Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die ausführbare Datei für das gewählte Programm angeben können, für die eine Dump-Datei angelegt werden soll.

   - **Tool starten**

     Wenn Sie auf diesen Link klicken, wird ein Fenster geöffnet, in dem Sie die ausführbare Datei für das gewählte Tool und die Einstellungen für den Start des Tools angeben können.

     Daraufhin wird das gewählte Tool auf dem Gerät heruntergeladen und gestartet.

Ereignisprotokolle downloaden

Um das Ereignisprotokoll von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Starten Sie das Tool für die Remote-Diagnose, und stellen Sie eine Verbindung mit dem gewünschten Gerät her.

2. Wählen Sie im Ordner **Ereignisprotokolle** des Objektbaumes des Geräts das gewünschte Protokoll aus, und klicken Sie im linken Fensterbereich des Tools für Remote-Diagnose auf den Link **Ereignisjournal Kaspersky Event Log downloaden**, um das Protokoll herunterzuladen.

Diagnose starten und Diagnoseergebnisse downloaden

Um die Diagnose für ein Programm auf einem Remote-Gerät zu starten und deren Ergebnisse herunterzuladen, gehen Sie wie folgt vor:

1. Starten Sie das Tool für die Remote-Diagnose, und stellen Sie eine Verbindung mit dem gewünschten Gerät her.

2. Wählen Sie im Objektbaum des Geräts das gewünschte Programm aus, und klicken Sie auf den Link **Diagnose ausführen**, um die Diagnose auszuführen.

   Daraufhin wird im Knoten für das gewählte Programm im Objektbaum der Diagnosebericht angezeigt.

3. Wählen Sie den erstellten Diagnosebericht im Objektbaum aus, und klicken Sie auf den Link **Datei downloaden**, um den Bericht herunterzuladen.

Starten, Beenden und Neustart von Programmen

Starten, Beenden und Neustart der Programme sind nur bei der Verbindung mit dem Gerät mittels Administrationsserver möglich.

Um eine Anwendung zu starten, zu beenden oder neu zu starten, gehen Sie wie folgt vor:

1. Starten Sie das Tool für die Remote-Diagnose, und stellen Sie eine Verbindung mit dem gewünschten Gerät her.
2. Wählen Sie im Objektbaum des Geräts das gewünschte Programm und im linken Fensterbereich eine Aktion aus:
   - **Programm beenden**
   - **Programm neu starten**
   - **Programm starten**.

   Je nach ausgewählter Aktion wird die Anwendung gestartet, beendet oder neu gestartet.

Benutzerkonten verwalten

Dieser Abschnitt enthält Informationen über die Benutzerkonten und Benutzerrollen, die vom Programm unterstützt werden. Es umfasst Anleitungen zur Erstellung von Benutzerkonten und Benutzerrollen für Kaspersky Security Center. Darüber hinaus enthält diese Abschnitt Anweisungen für die Arbeit mit Listen von Zertifikaten und mobilen Geräten des Benutzers sowie zum Versenden von Nachrichten an die Benutzer.

In diesem Abschnitt

Arbeiten mit Benutzerkonten

In Kaspersky Security Center können Benutzerkonten und Gruppen von Benutzerkonten verwaltet werden. Das Programm unterstützt zwei Typen von Konten:

- Benutzerkonten der Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Benutzerkonten dieser Benutzer beim Abfragen des Unternehmensnetzwerks.
- Benutzerkonten der internen Benutzer (s. Abschnitt "Arbeit mit internen Benutzern" auf S. 108). Werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Die Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center erstellt (s. Abschnitt "Benutzerkonten hinzufügen" auf S. 180) und verwendet.

Alle Benutzer können im Ordner **Benutzerkonten** der Konsolenstruktur angezeigt werden. Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

Mit Benutzerkonten und Benutzergruppen können folgenden Aktionen ausgeführt werden:

- Zugriffsrechte für die Funktionen des Programms mithilfe von Rollen konfigurieren (s. Abschnitt "Berechtigungen einrichten. Benutzerrollen" auf S. 185)
- Mithilfe von E-Mail oder SMS Benachrichtigungen an die Benutzer senden (s. Abschnitt "Nachrichten an die Benutzer versenden" auf S. 189)
- Liste der mobilen Geräte des Benutzers anzeigen (s. Abschnitt "Liste der mobilen Geräte des Benutzers anzeigen" auf S. 189)
- Zertifikate ausstellen und auf den mobilen Geräten des Benutzers installieren (s. Abschnitt "Benutzerzertifikat installieren" auf S. 190)
- Liste der für den Benutzer ausgestellten Zertifikate anzeigen (s. Abschnitt "Liste der für den Benutzer ausgestellten Zertifikate anzeigen" auf S. 191).

Benutzerkonten hinzufügen

Gehen Sie folgendermaßen vor, um ein neues Benutzerkonto für Kaspersky Security Center hinzuzufügen:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten**.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Öffnen Sie mithilfe der Schaltfläche **Benutzer hinzufügen** am Arbeitsplatz das Fenster **Eigenschaften**.

3. Geben Sie im Fenster **Eigenschaften** die Benutzerkonto-Einstellungen und das Kennwort ein, um eine Verbindung zu Kaspersky Security Center herzustellen.

   Das Kennwort muss lateinische Groß- und Kleinbuchstaben, Ziffern oder Sonderzeichen (@#$%^&*-_!+=[]{}|\\\\:',.?/`~()\\") enthalten. Die Länge des Kennworts muss mindestens acht und darf höchstens 16 Zeichen betragen.

   > Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Die Anzahl der Eingabeversuche für das Kennwort kann in der Registrierung mithilfe des Schlüssels SrvSplPpcLogonAttempts geändert werden.
   >
   > Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Konto des Benutzers für eine Stunde gesperrt. Der Administrator kann das Benutzerkonto nur durch die Änderung des Kennworts entsperren.

   Wenn das Kontrollkästchen **Konto deaktivieren** aktiviert ist, kann sich ein interner Benutzer (beispielsweise ein Benutzer mit Rechten eines Administrators oder Operators) nicht mit dem Programm verbinden. Sie können dieses Kontrollkästchen beispielsweise bei Kündigung eines Mitarbeiters aktivieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

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

Das erstellte Benutzerkonto wird im Arbeitsplatz des Ordners **Benutzerkonten** angezeigt.

Prüfung der Eindeutigkeit des Namens des internen Benutzers anpassen

Sie können die Prüfung der Eindeutigkeit des Namens des internen Benutzers von Kaspersky Security Center bei seinem Hinzufügen zum Programm anpassen. Die Prüfung der Eindeutigkeit des Namens des internen Benutzers kann nur auf dem virtuellen Server oder dem Hauptserver ausgeführt werden, für den das Benutzerkonto erstellt wird, bzw. auf allen virtuellen Servern und dem Hauptserver. Standardmäßig wird die Prüfung der Eindeutigkeit des Namens des internen Benutzers auf allen virtuellen Servern und auf dem Hauptadministrationsserver ausgeführt.

Um die Prüfung der Eindeutigkeit des Namens des internen Benutzers im Rahmen des virtuellen Servers oder des Hauptservers zu aktivieren, 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_InterUserUniqVsScope (DWORD) ist der Wert 00000001 festgelegt.

   Standardmäßig wird für diesen Schlüssel der Wert 0 festgelegt.
4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird die Prüfung der Namenseindeutigkeit nur auf jenem virtuellem Server ausgeführt, auf dem der interne Benutzer erstellt wurde, bzw. auf dem Hauptserver, wenn der Benutzer auf dem Hauptserver erstellt wurde.

Um die Prüfung der Eindeutigkeit des Namens des internen Benutzers auf allen virtuellen Servern und dem Hauptserver zu aktivieren, 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_InterUserUniqVsScope (DWORD) ist der Wert 00000000 festgelegt.

   Standardmäßig wird für diesen Schlüssel der Wert 0 festgelegt.

4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird die Prüfung der Eindeutigkeit des Namens des internen Benutzers auf allen virtuellen Servern und auf dem Hauptadministrationsserver ausgeführt.

Benutzergruppen hinzufügen

Sie können Gruppen hinzufügen und den Umfang der Gruppen sowie den Zugriff einer Benutzergruppe zu den verschiedenen Programmfunktionen flexibel konfigurieren. Die Benutzergruppen können einen ihrem Verwendungszweck entsprechenden Namen erhalten. Der Name kann beispielsweise dem Standort der Benutzer im Büro oder der Bezeichnung einer Unternehmensabteilung entsprechen, zu der die Benutzer gehören.

Ein Benutzer kann Teil mehrerer Benutzergruppen sein. Das Konto eines Benutzers unter der Verwaltung eines virtuellen Administrationsservers kann nur zu Benutzergruppen dieses virtuellen Servers gehören und verfügt nur über die im Rahmen dieses virtuellen Servers vorgesehenen Zugriffsrechte.

Um eine Benutzergruppe hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Klicken Sie auf die Schaltfläche **Sicherheitsgruppe hinzufügen**.

   Legen Sie im Fenster **Eigenschaften: Neue Gruppe** die Einstellungen der neu hinzugefügten Benutzergruppe fest.

3. Geben Sie im Abschnitt **Allgemein** den Namen der Gruppe an.

   Der Name der Gruppe darf nicht mehr als 100 Zeichen umfassen. Der Name der Gruppe muss eindeutig sein.

4. Fügen Sie im Abschnitt **Benutzer** die Benutzerkonten zur Gruppe hinzu.

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

Die hinzugefügte Benutzergruppe wird in der Konsolenstruktur im Ordner **Benutzerkonten** angezeigt.

Benutzer zur Gruppe hinzufügen

Gehen Sie folgendermaßen vor, um einen Benutzer zur Gruppe hinzuzufügen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** aus.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Wählen Sie in der Liste der Benutzerkonten und Gruppen die Gruppe, zu der ein Benutzer hinzugefügt werden soll.

3. Klicken Sie mit der rechten Maustaste auf die Gruppe, und wählen Sie **Eigenschaften** aus.

4. Wählen Sie im Eigenschaftsfenster der Gruppe den Abschnitt **Benutzer/Gruppe** aus und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

   Daraufhin wird ein Fenster mit einer Benutzerliste geöffnet.

5. Wählen Sie den oder die Benutzer, die zur Gruppe gehören sollen, aus der Liste aus.

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

Der Benutzer bzw. die Benutzer werden zur Gruppe hinzugefügt.

Berechtigungen einrichten. Benutzerrollen

Sie können den Zugriff von Administratoren, Benutzern und Benutzergruppen auf verschiedenen Programmfunktionen flexibel einrichten. Die Zugriffsberechtigung auf Programmfunktionen kann Benutzern auf zwei verschiedene Arten erteilt werden:

- Durch individuelle Konfiguration der Berechtigungen jedes Benutzers bzw. jeder Benutzergruppe.

- Durch Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und Zuweisung der Rollen an die Benutzer entsprechend ihrer dienstlichen Verpflichtungen.

Eine *Benutzerrolle* ist eine vordefinierte und vorkonfigurierte Sammlung von Zugriffsberechtigungen auf die Funktionen des Programms. Die Rolle kann einem Benutzer oder einer Benutzergruppe zugewiesen werden. Die Anwendung von Rollen vereinfacht und verkürzt die Routinearbeiten bei der Konfiguration von Zugriffsberechtigungen für Benutzer auf das Programm. Die Zugriffsberechtigungen werden in der Rolle entsprechend der "typischen" Aufgaben und dienstlichen Verpflichtungen des Benutzers festgelegt. Beispielsweise kann eine Benutzerrolle nur eine Leseberechtigung und eine Berechtigung zum Versenden von informativen Befehlen an mobile Geräte anderer Benutzer mithilfe des Self Service Portals enthalten.

Die Benutzerrollen können einen ihrem Verwendungszweck entsprechenden Namen erhalten. Es kann eine unbegrenzte Anzahl von Rollen erstellt werden.

Benutzerrollen hinzufügen

Um eine Benutzerrolle hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftsfenster des Administrationsservers den Abschnitt **Benutzerrollen** aus und klicken Sie auf die Schaltfläche **Hinzufügen**.

4. Passen Sie im Fenster **Eigenschaften: Neue Rolle** die Eigenschaften der Rolle an:

   - Geben Sie im Abschnitt **Allgemein** den Namen der Rolle an.

     Der Name der Rolle darf nicht mehr als 100 Zeichen umfassen.

   - Konfigurieren Sie im Abschnitt **Berechtigungen** die Berechtigungen, indem Sie neben den Programmfunktionen die Kontrollkästchen **Erlauben** und **Verbieten** aktivieren.

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

Die Rolle wird gespeichert.

Die für den Administrationsserver erstellten Benutzerrollen werden im Eigenschaftenfenster des Servers im Abschnitt **Benutzerrollen** angezeigt. Sie können Benutzerrollen ändern und löschen sowie Rollen Benutzergruppen zuweisen (s. Abschnitt "Benutzern oder Benutzergruppen eine Rolle zuweisen" auf S. 187) oder einzelnen Benutzern zuweisen.

> Der Abschnitt **Benutzerrollen** ist verfügbar, wenn im Fenster zur Anpassung der Benutzeroberfläche das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist. (s. Abschnitt "Benutzeroberfläche anpassen" auf S. 60)

Benutzern oder Benutzergruppen eine Rolle zuweisen

Gehen Sie wie folgt vor, um einem Benutzer oder einer Benutzergruppe eine Rolle zuzuweisen:

1. Wählen Sie in der Konsolenstruktur den Knoten mit dem Namen des gewünschten Administrationsservers aus.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers den Abschnitt **Sicherheit** aus.

4. Wählen Sie im Feld **Gruppen- oder Benutzernamen** den Benutzer oder die Benutzergruppe aus, dem bzw. der die Rolle zugewiesen werden soll.

   Wenn im Feld kein Benutzer bzw. keine Benutzergruppe angegeben ist, fügen Sie diese mithilfe der Schaltfläche **Hinzufügen** hinzu.

   Beim Hinzufügen eines Benutzers mithilfe der Schaltfläche **Hinzufügen** kann die Art der Benutzerauthentifizierung (Microsoft Windows oder Kaspersky Security Center) gewählt werden. Die Authentifizierung mittels Kaspersky Security Center wird bei der Auswahl von Benutzerkonten für interne Benutzer verwendet, die für die Arbeit mit virtuellen Administrationsservern genutzt werden.

5. Wechseln Sie zur Registerkarte **Rollen** und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Benutzerrollen** wird geöffnet. In diesem Fenster werden die erstellten Benutzerrollen angezeigt.

6. Wählen Sie im Fenster **Benutzerrollen** die Rolle für die Benutzergruppe aus.

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

Als Ergebnis wird dem Benutzer bzw. der Benutzergruppe die Rolle mit einer Auswahl von Berechtigungen für die Arbeit mit dem Administrationsserver zugewiesen. Die zugewiesenen Rollen werden im Eigenschaftsfenster des Administrationsservers auf der Registerkarte **Rollen** im Abschnitt **Sicherheit** angezeigt.

Der Abschnitt **Sicherheit** ist verfügbar, wenn im Fenster zur Anpassung der Benutzeroberfläche das Kontrollkästchen **Abschnitte mit Sicherheitseinstellungen anzeigen** aktiviert ist (s. Abschnitt "**Benutzeroberfläche anpassen**" auf S. 60).

Benutzer zum Eigentümer des Geräts bestimmen

Sie können einen Benutzer zum Eigentümer des Geräts bestimmen, um das Gerät unter diesem Benutzer zu "festigen". Sollte es erforderlich sein, bestimmte Aktionen mit dem Gerät auszuführen (beispielsweise ein Hardware-Update), kann der Administrator den Eigentümer des Geräts informieren und die Aktion mit ihm abstimmen.

Gehen Sie folgendermaßen vor, um einen Benutzer zum Geräteinhaber zu bestimmen:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verwaltete Geräte** aus.
2. Wählen Sie Im Arbeitsplatz auf der Registerkarte **Geräte** das Gerät aus, für das ein Eigentümer bestimmt werden soll.
3. Wählen Sie im Kontextmenü des Geräts den Punkt **Eigenschaften** aus.
4. Wählen Sie im Eigenschaftenfenster des Geräts den Abschnitt **Systeminformationen** → **Sitzungen** aus.
5. Klicken Sie auf die Schaltfläche **Zuweisen** neben dem Feld **Geräteinhaber**.
6. Wählen Sie im Fenster **Benutzer auswählen** den Benutzer aus, der zum Eigentümer des Geräts bestimmt werden soll, und klicken Sie auf die Schaltfläche **OK**.
7. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin wird der Geräteinhaber bestimmt. Das Feld **Geräteinhaber** enthält standardmäßig einen Wert aus Active Directory und wird bei jeder Abfrage von Active Directory aktualisiert (s. Abschnitt "Abfrageeinstellungen der Gruppe des Active Directory anzeigen und ändern" auf S. 213). Sie können sich eine Liste der Geräteinhaber im **Bericht über Geräteinhaber** anzeigen lassen. Der Bericht kann mithilfe des Assistenten für die Erstellung von Berichten erstellt werden (s. Abschnitt "Berichtsvorlage erstellen" auf S. 193).

Nachrichten an die Benutzer versenden

Gehen Sie folgendermaßen vor, um E-Mail-Nachrichten an Benutzer zu versenden:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzers die Option **Mitteilung per E-Mail senden**.

3. Füllen Sie im Fenster **Benutzernachricht** die erforderlichen Felder aus und klicken Sie auf die Schaltfläche **OK**.

Als Ergebnis wird eine Nachricht an die in den Eigenschaften des Benutzers angegebene E-Mail-Adresse gesendet.

Um eine SMS-Nachricht an den Benutzer zu versenden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

2. Wählen Sie im Kontextmenü des Benutzers die Option **SMS-Nachricht senden** aus.

3. Füllen Sie im Fenster **SMS-Text** die erforderlichen Felder aus und klicken Sie auf die Schaltfläche **OK**.

Als Ergebnis wird eine Nachricht an das mobile Gerät des Benutzers gesendet, dessen Nummer in den Eigenschaften des Benutzers angegeben ist.

Liste der mobilen Geräte des Benutzers anzeigen

Um eine Liste der mobilen Geräte anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Benutzerkontos den Abschnitt **Mobile Geräte** aus.

Im Abschnitt **Mobile Geräte** werden eine Liste der mobilen Geräte des Benutzers sowie Informationen über die mobilen Geräte angezeigt. Durch Klicken auf die Schaltfläche **In Datei exportieren** kann die Liste der mobilen Geräte in einer Datei gespeichert werden.

Benutzerzertifikat installieren

Sie können für einen Benutzer drei Arten von Zertifikaten installieren:

- Allgemeine Zertifikate zur Identifikation des mobilen Geräts des Benutzers
- E-Mail-Zertifikate für die Einrichtung der Unternehmens-E-Mail auf dem mobilen Gerät des Benutzers
- VPN-Zertifikate für die Einrichtung eines virtuellen privaten Netzwerks auf dem mobilen Gerät des Benutzers

Gehen Sie wie folgt vor, um für einen Benutzer ein Zertifikat auszustellen und zu installieren:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Benutzerkonten** und wählen Sie ein Benutzerkonto aus.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Zertifikat installieren** aus.

Der Assistent zur Zertifikatinstallation wird gestartet. Folgen Sie den Anweisungen.

Als Ergebnis der Ausführung des Assistenten zur Zertifikatinstallation wird ein Zertifikat für den Benutzer erstellt und installiert. Eine Liste der für den Benutzer installierten Zertifikate kann angezeigt und in eine Datei exportiert werden (s. Abschnitt "Liste der für den Benutzer ausgestellten Zertifikate anzeigen" auf S. 191).

Liste der für den Benutzer ausgestellten Zertifikate

Um eine Liste aller für den Benutzer ausgestellten Zertifikate anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Benutzerkonten** den Benutzer aus.

   Der Ordner **Benutzerkonten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Wählen Sie im Kontextmenü des Benutzerkontos die Option **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Benutzerkontos den Abschnitt **Zertifikate** aus.

Im Abschnitt **Zertifikate** werden eine Liste der Zertifikate des Benutzers sowie Informationen zu den Zertifikaten angezeigt. Durch Klicken auf die Schaltfläche **In Datei exportieren** können Sie die Liste der Zertifikate in einer Datei speichern.

Berichte, Statistiken und Benachrichtigungen

Diesem Abschnitt können Sie Informationen über die Arbeit mit Berichten, Statistiken und Ereignis- und Geräteauswahlen in Kaspersky Security Center sowie über die Konfiguration der Administrationsserver-Benachrichtigungen entnehmen.

In diesem Abschnitt

Berichte

Berichte in Kaspersky Security Center enthalten Informationen über den Zustand der verwalteten Geräte. Berichte werden anhand der Daten erstellt, die auf dem Administrationsserver gespeichert werden. Sie können Berichte für folgende Objekte erstellen:

- für Auswahlen von Geräten, die nach bestimmten Parametern erstellt wurden
- für Administrationsgruppen
- für bestimmte Geräte aus verschiedenen Administrationsgruppen
- für alle Geräte im Netzwerk (im Bericht über die Softwareverteilung).

Das Programm verfügt über eine Auswahl von Standard-Berichtsvorlagen. Ferner gibt es die Möglichkeit zum Erstellen von benutzerdefinierten Berichtsvorlagen. Berichte werden im Programmhauptfenster im Ordner **Administrationsserver** der Konsolenstruktur angezeigt.

In diesem Abschnitt

Berichtsvorlage erstellen

Um eine Berichtsvorlage zu erstellen, 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. Klicken Sie auf die Schaltfläche **Berichtsvorlage erstellen**.

   Daraufhin wird der Assistent für das Erstellen einer Berichtsvorlage gestartet. Folgen Sie den Anweisungen.

Nach Abschluss des Assistenten wird die erstellte Berichtsvorlage zum ausgewählten Ordner **Administrationsserver** der Konsolenstruktur hinzugefügt. Diese Vorlage kann nun zum Erstellen und Anzeigen von Berichten verwendet werden.

Berichte erstellen und anzeigen

Um einen Bericht zu erstellen und 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 aus der Vorlagenliste die gewünschte Vorlage aus.

   Daraufhin wird im Arbeitsplatz der Bericht angezeigt, der nach der gewählten Vorlage erstellt wurde.

Im Bericht werden folgende Daten angezeigt:

- Typ und Name des Berichts, dessen Kurzbeschreibung und Berichtszeitraum sowie Informationen darüber, für welche Gerätegruppe der Bericht erstellt wurde

- Diagramm mit den meisten typischen Berichtsdaten

- Übersichtstabelle mit Kennziffern des Berichts.
- Tabelle mit detaillierten Daten des Berichts.

Bericht speichern

Um den erstellten Bericht zu speichern, 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 aus der Vorlagenliste die gewünschte Vorlage aus.
4. Klicken Sie mit der rechten Maustaste auf die gewählte Berichtsvorlage und wählen Sie **Speichern** aus.

Daraufhin wird der Assistent zur Berichtspeicherung gestartet. Folgen Sie den Anweisungen.

Nach Abschluss des Assistenten wird der Ordner geöffnet, in dem die Berichtsdatei gespeichert wurde.

Aufgabe zum Berichtsversand anlegen

Berichte können per E-Mail versendet werden. Der Versand von Berichten erfolgt in Kaspersky Security Center mithilfe der Aufgabe Berichtsversand.

Um eine Aufgabe für den Versand eines einzelnen Berichts zu erstellen, 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 aus der Liste der Berichte die gewünschte Vorlage aus.
4. Klicken Sie mit der rechten Maustaste auf die Berichtsvorlage und wählen Sie **Berichte senden** aus.

Daraufhin wird der Assistent für die Erstellung einer Aufgabe zum Berichtsversand gestartet. Folgen Sie den Anweisungen.

Um eine Aufgabe für den Versand von mehreren Berichten anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Knoten mit dem Namen des gewünschten Administrationsservers den Ordner **Aufgaben**.

2. Klicken Sie im Arbeitsplatz des Ordners **Aufgaben** auf die Schaltfläche **Aufgabe erstellen**.

Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen. Wählen Sie im Fenster des Assistenten **Aufgabentyp** den Aufgabentyp **Berichtsversand** aus.

Die erstellte Aufgabe Berichtsversand wird im Ordner **Aufgaben** der Konsolenstruktur angezeigt.

Die Aufgabe Berichtsversand wird automatisch erstellt, sofern bei der Installation von Kaspersky Security Center die E-Mail-Einstellungen angegeben wurden (s. Abschnitt "Schnellstartassistent für den Administrationsserver" auf S. 75).

Statistik

Statistische Informationen über den Zustand des Schutzsystems und der verwalteten Geräte wird im Arbeitsplatz des Knotens **Administrationsserver** auf der Registerkarte **Statistik** angezeigt. Die Registerkarte **Statistik** enthält mehrere untergeordnete Registerkarten (Seiten). Auf jeder Seite werden Informationsbereiche mit statistischen Informationen angezeigt. Statistikdaten werden in den Informationsbereichen als Kreis- oder Säulendiagramme oder Tabellen dargestellt. Daten in den Informationsbereichen werden während der Ausführung des Programms aktualisiert und spiegeln den aktuellen Status des Schutzprogramms wieder.

Sie können die Zusammenstellung der auf der Registerkarte **Statistik** enthaltenen Seiten, die Auswahl der Informationsbereiche auf jeder Seite sowie die Darstellungsweise der Daten in den Informationsbereichen ändern.

*Um auf der Registerkarte **Statistik** eine neue Seite mit Informationsbereichen hinzuzufügen, gehen Sie folgendermaßen vor:*

1. Klicken Sie auf die Schaltfläche **Ansicht einstellen** in der rechten oberen Ecke der Registerkarte **Statistik**.

   Daraufhin wird das Fenster **Eigenschaften: Statistik** geöffnet. Dieses Fenster enthält eine Liste von Seiten, die derzeit auf der Registerkarte **Statistik** enthalten sind. Sie können im Fenster die Anzeigereihenfolge der Fenster auf der Registerkarte ändern, Seiten hinzufügen und entfernen und mithilfe der Schaltfläche **Eigenschaften** zu den Seiteneigenschaften wechseln.

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

   Daraufhin wird das Eigenschaftenfenster der neuen Seite geöffnet.

3. Konfigurieren Sie die neue Seite:

   - Geben Sie im Abschnitt **Allgemein** den Namen der Seite an.
   - Fügen Sie im Abschnitt **Informationsbereiche** mithilfe der Schaltfläche **Hinzufügen** Informationsbereiche hinzu, die auf der Seite angezeigt werden sollen.

     Mithilfe der Schaltfläche **Eigenschaften** im Abschnitt **Informationsbereiche** können Sie die Eigenschaften der hinzugefügten Informationsbereiche anpassen: Name, Typ und Art des Diagramms im Bereich, Daten für die Erstellung des Diagramms.

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

Die hinzugefügte Seite mit Informationsbereichen wird auf der Registerkarte **Statistik** angezeigt. Mithilfe der Schaltfläche  können Sie rasch zwischen der Seitenkonfiguration und dem ausgew,ählten Informationsbereich auf der Seite wechseln.

Benachrichtigungseinstellungen für Ereignisse anpassen

Kaspersky Security Center ermöglicht die Auswahl der Benachrichtigungsmethode für Ereignisse für den Administrator auf den Client-Geräten und die Anpassung der Benachrichtigungseinstellungen:

- E-Mail. Beim Auftreten eines Ereignisses sendet das Programm Benachrichtigungen an die angegebenen E-Mail-Adressen. Der Text der Benachrichtigung kann angepasst werden.
- SMS. Beim Auftreten eines Ereignisses sendet das Programm Benachrichtigungen an die angegebenen Telefonnummern. Sie können den SMS-Versand über ein E-Mail-Gateway oder mithilfe des Tools Kaspersky SMS Broadcasting einrichten.
- Ausführbare Datei Beim Auftreten eines Ereignisses auf dem Gerät wird auf dem Administrator-Arbeitsplatz eine ausführbare Datei gestartet.
  Mithilfe der ausführbaren Datei erhält der Administrator die Parameter des eingetretenen Ereignisses (s. Abschnitt "Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei" auf S. 385).

Um die Einstellungen für Benachrichtigungen über Ereignisse auf den Client-Geräten anzupassen, 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 **Ereignisse** aus.
3. Wählen Sie mithilfe des Links **Benachrichtigungseinstellungen und Ereignis-Export anpassen** in der Dropdown-Liste die Option **Benachrichtigungseinstellungen anpassen**.

   Daraufhin wird das Fenster **Eigenschaften: Ereignisse** geöffnet.
4. Wählen Sie im Abschnitt **Benachrichtigung** eine Benachrichtigungsmethode aus (E-Mail, SMS, ausführbare Startdatei) und passen Sie die Benachrichtigungseinstellungen an.
5. Geben Sie im Feld **Benachrichtigungstext** den Text ein, den das Programm bei Eintreten eines Ereignisses versenden wird.

Aus der Dropdown-Liste rechts vom Textfeld können in die Nachricht Platzhalter für zusätzliche Einstellungen mit den Ereignisdetails (wie Beschreibung, Eintrittszeit des Ereignisses und sonstiges) hinzugefügt werden.

> Wenn der Benachrichtigungstext das Zeichen % enthält, muss es zweimal angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Der Prozessordownload beträgt 100%%".

6. Überprüfen Sie über die Schaltfläche **Testnachricht senden**, ob die Benachrichtigungen richtig eingestellt wurden.

   Das Programm sendet eine Testbenachrichtigung an den angegebenen Empfänger.

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

Daraufhin werden die angepassten Einstellungen der Benachrichtigung auf alle Ereignisse übernommen, die auf den Client-Geräten auftreten.

Sie können Benachrichtigungen über Ereignisse auch schnell im Eigenschaftenfenster des Ereignisses konfigurieren, indem Sie auf die Links **Ereigniseinstellungen für Kaspersky Endpoint Security anpassen** oder **Ereigniseinstellungen des Administrationsservers anpassen** klicken.

Siehe auch:

Ereignisse auf dem Administrationsserver verarbeiten und speichern..... 106

Zertifikat für SMTP-Server erstellen

Um ein Zertifikat für einen SMTP-Server zu erstellen, 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 **Ereignisse** aus.

3. Wählen Sie mithilfe des Links **Benachrichtigungseinstellungen und Ereignis-Export anpassen** in der Dropdown-Liste die Option **Benachrichtigungseinstellungen anpassen**.

   Das Eigenschaftenfenster des Ereignisses wird geöffnet.

4. Wählen Sie auf der Registerkarte **E-Mail** mithilfe des Links **Einstellungen** das Fenster **Einstellungen**.

5. Öffnen Sie im Fenster **Einstellungen** mithilfe des Links **Angabe des Zertifikats** das Fenster **Zertifikat für die Signatur**.

6. Klicken Sie im Fenster **Zertifikat für die Signatur** auf die Schaltfläche **Festlegen**.

   Daraufhin öffnet sich das Fenster **Zertifikat**.

7. Wählen Sie im Dropdown-Feld **Zertifikatstyp** entweder einen offenen oder geschlossenen Zertifikatstyp aus.

   - Wenn ein geschlossener Zertifikatstyp ausgewählt ist (**Container PKCS#12**), geben Sie die Zertifikatsdatei und das Kennwort an.

   - Wenn ein offener Zertifikatstyp ausgewählt ist (**X.509-Zertifikat**):

     a. Geben Sie die Datei des privaten Schlüssels an (Datei mit der Erweiterung prk oder pem).

     b. Geben Sie das Kennwort des privaten Schlüssels an.

     c. Geben Sie die Datei des offenen Schlüssel an (Datei mit der Erweiterung cer).

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

Daraufhin wird ein Zertifikat für den SMTP-Server ausgestellt.

Ereignisauswahlen

Informationen über die von Kaspersky Security Center registrierten Ereignisse und verwalteten Programme werden im Microsoft-Windows-Systemprotokoll und im Ereignisprotokoll von Kaspersky Security Center gespeichert. Sie können die Informationen aus dem Ereignisprotokoll für Kaspersky Security Center im Arbeitsplatz des Knotens **Administrationsserver** auf der Registerkarte **Ereignisse** anzeigen lassen.

Die Informationen auf der Registerkarte **Ereignisse** werden in Form einer Liste mit Ereignisauswahlen angezeigt. Jede Auswahl umfasst nur Ereignisse eines bestimmten Typs. Beispielsweise enthält die Auswahl "Gerätestatus – Kritisch" nur Einträge über Änderungen des Gerätestatus auf "Kritisch". Nach der Installation des Programms sind auf der Registerkarte **Ereignisse** eine Reihe von Standardauswahlen für Ereignisse enthalten. Sie können zusätzliche (benutzerdefinierte) Ereignisauswahlen erstellen sowie Informationen über Ereignisse in eine Datei exportieren.

In diesem Abschnitt

Ereignisauswahl anzeigen

Um sich eine Ereignisauswahl anzeigen zu lassen, 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 **Ereignisse** aus.
3. Wählen Sie in der Dropdown-Liste **Ereignisse für Auswahl** die gewünschte Ereignisauswahl aus.

   Wenn Sie möchten, dass die Ereignisse dieser Auswahl ständig im Arbeitsplatz angezeigt wird, klicken Sie auf die Schaltfläche ☆ neben der Auswahl.

Daraufhin wird im Arbeitsplatz die Liste der Ereignisse des gewählten Typs angezeigt, die auf dem Administrationsserver gespeichert werden.

Sie können die Informationen in der Ereignisliste in einer beliebigen Spalte der Liste in auf- oder absteigender Reihenfolge sortieren.

Einstellungen für Ereignisauswahl anpassen

Um die Einstellungen für eine Ereignisauswahl anzupassen, 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 **Ereignisse** aus.
3. Öffnen Sie die gewünschte Ereignisauswahl auf der Registerkarte **Ereignisse**.
4. Klicken Sie auf die Schaltfläche **Auswahleigenschaften**.

Im folgenden Eigenschaftenfenster der Ereignisauswahl können Sie die Einstellungen der Auswahl anpassen.

Ereignisauswahl erstellen

Um eine Ereignisauswahl zu erstellen, 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 **Ereignisse** aus.

3. Klicken Sie auf die Schaltfläche **Auswahl erstellen**.

4. Geben Sie im folgenden Fenster **Neue Ereignisauswahl** den Namen der zu erstellenden Auswahl an, und klicken Sie auf **OK**.

   Daraufhin wird in der Dropdown-Liste **Ereignisauswahlen** eine Auswahl mit dem von Ihnen angegebenen Namen erstellt.

Die erstellte Ereignisauswahl enthält standardmäßig alle Ereignisse,
die auf dem Administrationsserver gespeichert werden. Damit bestimmte Ereignisse
in der Auswahl angezeigt werden, konfigurieren Sie die Einstellungen der Auswahl.

Ereignisauswahl in eine Textdatei exportieren

Um eine Ereignisauswahl in eine Datei zu exportieren, 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 **Ereignisse** aus.

3. Klicken Sie auf die Schaltfläche **Import/Export**.

4. Wählen Sie in der Dropdown-Liste die Option **Ereignisse in Datei exportieren**.

   Daraufhin wird der Assistent für den Ereignis-Export gestartet. Folgen Sie den Anweisungen.

Ereignisse aus einer Auswahl löschen

Um Ereignisse aus der Auswahl zu löschen, 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 **Ereignisse** aus.
3. Wählen Sie mit der Maus und den Tasten **Umschalt** oder **Strg** Ereignisse aus, die gelöscht werden sollen.
4. Löschen Sie die gewählten Ereignisse auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf ein beliebiges Ereignis und wählen Sie **Entfernen**.

     Mit der Auswahl **Alle löschen** werden aus der Auswahl alle angezeigten Ereignisse gelöscht, und zwar unabhängig davon, welche Ereignisse zuvor zum Löschen gewählt wurden.

   - Klicken Sie im Block mit den gewählten Ereignissen auf den Link **Ereignis löschen**, wenn ein einziges Ereignis gewählt wurde, oder auf den Link **Ereignisse löschen**, wenn mehrere Ereignisse gewählt wurden.

Daraufhin werden die ausgewählten Ereignisse gelöscht.

Ereignisse in das SIEM-System exportieren

Das Programm ermöglicht den Export von Ereignissen bei der Ausführung des Administrationsservers und anderer auf den Client-Geräten installierter Kaspersky-Lab-Programme in das SIEM-System (SIEM steht für Security Information and Event Management).

Um den Export der Ereignisse in das SIEM-System anzupassen, 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 **Export in das SIEM-System anpassen**.

   Das Eigenschaftenfenster für Ereignisse wird im Abschnitt **Ereignisexport** geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Ereignisse automatisch in die Datenbank des SIEM-Systems exportieren**.

5. Wählen Sie in der Dropdown-Liste **SIEM-System** das System, in das die Ereignisse exportiert werden sollen.

   Der Export ist in die SIEM-Systeme QRadar (leef-Format), ArcSight (cef-Format), Splunk (cef-Format) und Syslog (RFC 5424) möglich. Standardmäßig ist das System ArcSight (cef-Format) ausgewählt.

6. Geben Sie in den entsprechenden Feldern die Serveradresse und den Port für die Verbindung mit dem Server des SIEM-Systems an.

   Mithilfe der Schaltfläche **Archiv exportieren** werden bereits erstellte Ereignisse ab dem angegebenen Datum in die Datenbank des SIEM-Systems exportiert. Standardmäßig werden Ereignisse an dem aktuellen Datum exportiert.

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

Daraufhin werden nach der Aktivierung des Kontrollkästchens **Ereignisse automatisch in die Datenbank des SIEM-Systems exportieren** und dem Aufbau einer Verbindung mit dem Server des Programms alle Ereignisse während der Ausführung des Administrationsservers und anderer Programme von Kaspersky Lab automatisch in das SIEM-System exportiert.

Ausführliche Informationen über den Export von Ereignissen finden Sie in der Online-Hilfe der Webressource von Kaspersky Lab https://click.kaspersky.com/?hl=en-US&link=online_help&pid=KSCEventExport&version=1.0&helpid=.

Geräteauswahlen

Informationen zum Status der Geräte und mobiler Geräte finden Sie in der Konsolenstruktur im Ordner **Geräteauswahlen**.

Die Informationen im Ordner **Geräteauswahlen** sind in Form einer Liste der Geräteauswahlen dargestellt. Jede Auswahl beinhaltet Geräte, die bestimmten Bedingungen entsprechen. Beispielsweise enthält die Auswahl **Geräte mit dem Status "Kritisch"** nur die Geräte mit dem Status *Kritisch*. Nach Installation des Programms wird in dem Ordner **Geräteauswahlen** eine Reihe von Standardauswahlen angezeigt. Sie können zusätzliche (benutzerdefinierte) Geräteauswahlen erstellen, Einstellungen für Auswahlen in eine Datei exportieren und Auswahlen mit den aus einer Datei importierten Einstellungen erstellen.

In diesem Abschnitt

Geräteauswahl anzeigen

Um eine Geräteauswahl anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Wählen Sie im Arbeitsplatz des Ordners aus der Dropdown-Liste **Geräte der Auswahl** die gewünschte Geräteauswahl.

Wenn Sie möchten, dass die Geräte dieser Auswahl ständig im Arbeitsplatz angezeigt wird, klicken Sie auf die Schaltfläche ☆ neben der Auswahl.

Daraufhin wird im Arbeitsplatz die Liste der Geräte angezeigt, die den Einstellungen der Auswahl entsprechen.

Sie können die Informationen in der Geräteliste in einer beliebigen Spalte in auf- oder absteigender Reihenfolge sortieren.

Einstellungen einer Geräteauswahl anpassen

Um die Einstellungen für eine Geräteauswahl anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Wählen Sie die gewünschte Geräteauswahl aus.
3. Klicken Sie auf die Schaltfläche **Auswahleigenschaften**.
4. Passen Sie im folgenden Eigenschaftenfenster die allgemeinen Eigenschaften der Auswahl und die Kriterien für die Zugehörigkeit von Geräten zur Auswahl an.
5. Klicken Sie auf die Schaltfläche **OK**.

Geräteauswahl erstellen

Um eine Geräteauswahl zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Klicken Sie im Arbeitsplatz des Ordners auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Auswahl erstellen**.
3. Geben Sie im folgenden Fenster **Neue Geräteauswahl** den Namen der zu erstellenden Auswahl an, und klicken Sie auf **OK**.

Daraufhin wird in der Konsolenstruktur im Ordner **Geräteauswahlen** ein neuer Ordner mit dem angegebenen Namen angelegt. Die erstellte Geräteauswahl enthält standardmäßig alle Geräte, die zu den Administrationsgruppen des Servers gehören, der die Auswahl verwaltet. Damit bestimmte Geräte in der Auswahl angezeigt werden, konfigurieren Sie mithilfe der Schaltfläche **Auswahleigenschaften** die Einstellungen der Auswahl.

Einstellungen einer Geräteauswahl in eine Datei exportieren

Um die Einstellungen einer Geräteauswahl in eine Datei zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.

2. Klicken Sie im Arbeitsplatz des Ordners auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Einstellungen exportieren**.

3. Geben Sie im folgenden Fenster **Speichern unter** den Namen für die Exportdatei der Auswahleinstellungen ein, geben Sie einen Ordner an, in dem die Datei gespeichert werden soll, und klicken Sie auf die Schaltfläche **Speichern**.

Die Einstellungen der Geräteauswahl werden in der angegebenen Datei gespeichert.

Geräteauswahl mit importierten Einstellungen erstellen

Um eine Geräteauswahl mit importierten Einstellungen zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.

2. Klicken Sie im Arbeitsplatz des Ordners auf die Schaltfläche **Erweitert** und wählen Sie in der Dropdown-Liste die Option **Importieren**.

3. Geben Sie im folgenden Fenster den Pfad der Datei an, aus der die Auswahleinstellungen importiert werden sollen. Klicken Sie auf **Öffnen**.

Daraufhin wird im Ordner **Geräteauswahlen** die Auswahl **Neue Auswahl** erstellt, deren Einstellungen aus der angegeben Datei importiert wurden.

> Wenn im Ordner **Geräteauswahlen** eine Auswahl mit dem Namen **Neue Auswahl** bereits vorhanden ist, wird dem Namen der erstellten Auswahl eine Endung der Form **(<laufende Nummer>)** angehängt. Beispiel: **(1)**, **(2)**.

Geräte in der Auswahl aus Administrationsgruppen löschen

Bei der Arbeit mit einer Geräteauswahl können Sie Geräte direkt in der Auswahl aus den Administrationsgruppen löschen, ohne auf die Administrationsgruppen zu wechseln, aus denen die Geräte gelöscht werden sollen.

Um Geräte aus Administrationsgruppen zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Geräteauswahlen** aus.
2. Wählen Sie die Geräte aus, die gelöscht werden sollen. Drücken Sie dazu die Taste **Umschalt** oder **Strg**.
3. Löschen Sie die gewählten Geräte aus den Administrationsgruppen auf eine der folgenden Weisen:
   - Klicken Sie mit der rechten Maustaste auf eines der gewählten Geräte und wählen Sie **Entfernen** aus.
   - Klicken Sie auf die Schaltfläche **Aktion ausführen** und wählen Sie in der Dropdown-Liste die Option **Aus der Gruppe löschen**.

Daraufhin werden die gewählten Geräte aus den Administrationsgruppen gelöscht, zu denen sie gehörten.

Richtlinien

Informationen über Richtlinien sind im Ordner **Richtlinien** enthalten.

Im Ordner **Richtlinien** wird eine Liste der in den Administrationsgruppen erstellten Richtlinien angezeigt. Nach der Programminstallation enthält der Ordner eine Liste der automatisch erstellten Richtlinien. Sie können die Richtlinienliste aktualisieren, Richtlinien erstellen sowie die Eigenschaften der in der Liste ausgewählten Richtlinie anzeigen.

Das Diagramm zeigt den Fortschritt der Anwendung der Richtlinie auf den Client-Geräten, für die diese bestimmt ist. Wenn sich die Farbe des Diagramms vollständig zu Grün ändert, bedeutet es, dass die Richtlinie auf allen Client-Geräten angewandt wurde.

Aufgaben

Informationen über Aufgaben sind im Ordner **Aufgaben** enthalten.

Im Ordner **Aufgaben** wird eine Liste der Aufgaben angezeigt, die den Client-Geräten in den Administrationsgruppen und dem Administrationsserver zugewiesen wurden. Nach der Programminstallation enthält der Ordner eine Liste der automatisch erstellten Aufgaben. Sie können die Aufgabenliste aktualisieren, Aufgaben erstellen und die Eigenschaften der Aufgaben anzeigen sowie Aufgaben starten und anhalten.

Nicht zugeordnete Geräte

Dieser Abschnitt enthält Informationen zur Arbeit mit Geräten im Firmennetzwerk, die nicht zur Administrationsgruppe gehören.

In diesem Abschnitt

Netzwerkabfrage

Der Administrationsserver empfängt die Daten über die Netzwerkstruktur und deren Geräte, indem das Windows-Netzwerk, die IP-Bereiche und das Active Directory im Unternehmensnetzwerk regelmäßig durchsucht werden. Anhand der Ergebnisse wird der Inhalt des Ordners **Nicht zugeordnete Geräte** aktualisiert.

Der Administrationsserver kann folgende Arten von Netzwerkabfragen durchführen:

- **Windows-Netzwerkabfrage**. Es gibt zwei Arten der Windows-Netzwerkabfrage: Schnellabfrage und Komplettabfrage. Bei der Schnellabfrage empfängt der Server nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. Während einer Komplettabfrage werden von jedem Client-Gerät folgende Informationen abgefragt: Betriebssystem, IP-Adresse, DNS, NetBIOS.

- **IP-Bereiche durchsuchen**. Der Administrationsserver durchsucht jetzt die erstellten IP-Bereiche mit ICMP-Paketen und ruft alle Daten über die Geräte ab, die zu den IP-Bereichen gehören.

- **Abfrage der Active Directory-Gruppen**. Dabei werden in die Datenbank des Administrationsservers Informationen über die Struktur der Active Directory Gruppen sowie über die DNS-Namen der Geräte eingetragen, die zu Active Directory Gruppen gehören.

Auf Grundlage der empfangenen Daten und der Daten über die Struktur des Firmennetzwerks aktualisiert Kaspersky Security Center den Inhalt der Ordner **Nicht zugeordnete Geräte** und **Verwaltete Geräte**. Wenn in einem Firmennetzwerk das automatische Verschieben von Geräten in Administrationsgruppen eingestellt wurde, werden die im Netzwerk gefundenen Geräte in Administrationsgruppen aufgenommen.

In diesem Abschnitt

Einstellungen der Windows-Netzwerkabfrage anzeigen und ändern

Um die Einstellungen der Windows-Netzwerkabfrage zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **Domänen**.

   Sie können zum Ordner **Netzwerkabfrage** aus dem Ordner **Nicht zugeordnete Geräte** wechseln, indem Sie auf die Schaltfläche **Jetzt abfragen** klicken.

2. Klicken Sie im Arbeitsplatz des Ordners **Domänen** auf die Schaltfläche **Einstellungen der Abfrage anpassen**.

Daraufhin öffnet sich das Fenster **Eigenschaften: Domänen**, in dem Sie die Einstellungen für die Windows-Netzwerkabfrage anzeigen und anpassen können.

> Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Update-Agenten im Abschnitt **Netzwerkabfrage** die Einstellungen für die Windows-Netzwerkabfrage anzeigen und ändern.

Abfrageeinstellungen der Gruppe des Active Directory anzeigen und ändern

Um die Abfrageeinstellungen der Gruppe des Active Directory zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **Active Directory**.

   Sie können zum Ordner **Netzwerkabfrage** aus dem Ordner **Nicht zugeordnete Geräte** wechseln, indem Sie auf die Schaltfläche **Jetzt abfragen** klicken.

2. Öffnen Sie über den Link **Einstellungen der Abfrage anpassen** das Fenster **Eigenschaften: Active Directory**.

Im Fenster **Eigenschaften: Active Directory** können Sie die Einstellungen für die Abfrage der Active Directory-Gruppen anzeigen und anpassen.

Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Update-Agenten im Abschnitt **Netzwerkabfrage** die Einstellungen zur Abfrage der Gruppen des Active Directory anzeigen und ändern.

Einstellungen für die Abfrage der IP-Bereiche anzeigen und ändern

Um die Einstellungen der Abfrage für den IP-Bereich zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **IP-Bereiche**.

   Sie können zum Ordner **Netzwerkabfrage** aus dem Ordner **Nicht zugeordnete Geräte** wechseln, indem Sie auf die Schaltfläche **Jetzt abfragen** klicken.

2. Öffnen Sie über den Link **Einstellungen der Abfrage anpassen** das Fenster **Eigenschaften: IP-Bereiche**.

Im Fenster **Eigenschaften: IP-Bereiche** können Sie die Einstellungen der Abfrage für IP-Bereiche einsehen und ändern.

Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Update-Agenten im Abschnitt **Netzwerkabfrage** die Einstellungen für die Abfrage der IP-Bereiche anzeigen und ändern. Die Client-Geräte, die während der Abfrage der IP-Bereiche gefunden wurden, werden im Ordner **Domänen** des virtuellen Servers angezeigt.

Arbeit mit Windows-Domänen. Domäneneinstellungen anzeigen und ändern

Um die Einstellungen einer Domäne zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **Domänen**.

2. Wählen Sie eine Domäne aus, und öffnen Sie das Eigenschaftenfenster der Domäne auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Domäne, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf den Link **Gruppeneigenschaften anzeigen**.

   Daraufhin wird das Fenster **Eigenschaften: <Domänenname>** geöffnet, in dem Sie die Einstellungen der gewählten Domäne anpassen können.

IP-Bereiche

Sie können die Einstellungen der vorhandenen IP-Bereiche anpassen und neue IP-Bereiche erstellen.

In diesem Abschnitt

IP-Bereich erstellen

Um einen IP-Bereich zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **IP-Bereiche**.

2. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen **Erstellen** → **IP-Bereich**.

3. Konfigurieren Sie im folgenden Fenster **Neuer IP-Bereich** die Einstellungen des zu erstellenden IP-Bereichs.

Daraufhin wird der neue IP-Bereich im Ordner **IP-Bereiche** angezeigt.

Einstellungen eines IP-Bereichs anzeigen und ändern

Um die Einstellungen der Abfrage eines IP-Bereichs anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **IP-Bereiche**.

2. Wählen Sie einen IP-Bereich aus, und öffnen Sie sein Eigenschaftenfenster auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf den IP-Bereich und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf den Link **Gruppeneigenschaften anzeigen**.

Daraufhin wird das Fenster **Eigenschaften: <Name des IP-Bereichs>** geöffnet, in dem Sie die Einstellungen des gewählten IP-Bereichs anpassen können.

Active Directory Gruppen. Gruppeneinstellungen anzeigen und ändern

Um die Einstellungen einer Gruppe des Active Directory zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Netzwerkabfrage** den Unterordner **Active Directory**.

2. Wählen Sie die erforderliche Gruppe des Active Directory, und öffnen Sie das Eigenschaftenfenster der Gruppe auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Gruppe, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf den Link **Gruppeneigenschaften anzeigen**.

   Daraufhin wird das Fenster **Eigenschaften: <Name der Gruppe des Active Directory>** geöffnet, in dem Sie die Einstellungen der gewählten Gruppe des Active Directory anpassen können.

Regeln für das automatische Verschieben von Geräten in Administrationsgruppen erstellen

Sie können das automatische Verschieben von Geräten, die während der Abfrage des Firmennetzwerks gefunden werden, in Administrationsgruppen einstellen.

Um die Regeln für das automatische Verschieben von Geräten in Administrationsgruppen festzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Nicht zugeordnete Geräte** aus.

2. Klicken Sie im Arbeitsplatz des Ordners auf die Schaltfläche **Regeln anpassen**.

Daraufhin wird das Fenster **Eigenschaften: Nicht zugeordnete Geräte** geöffnet. Konfigurieren Sie die Regeln für das automatische Verschieben von Geräten in Administrationsgruppen im Abschnitt **Geräte verschieben**.

Dynamischen VDI-Modus auf Client-Geräten verwenden

Im Netzwerk eines Unternehmens kann eine virtuelle Infrastruktur mit befristeter Nutzung virtueller Maschinen bereitgestellt werden. Kaspersky Security Center erkennt temporäre virtuelle Maschinen und fügt ihre Daten zur Datenbank des Administrationsservers hinzu.
Nachdem der Benutzer seine Arbeit auf der temporären virtuellen Maschine beendet hat, wird die virtuelle Maschine aus der virtuellen Infrastruktur entfernt. Der Eintrag der virtuellen Maschine kann jedoch in der Datenbank des Administrationsservers gespeichert werden. Darüber hinaus können nicht vorhandene virtuelle Maschinen in der Verwaltungskonsole angezeigt werden.

Damit keine Daten über nicht vorhandene virtuelle Maschinen gespeichert werden, wurde in Kaspersky Security Center die Unterstützung des dynamischen Modus für die Virtual Desktop Infrastructure (VDI) realisiert. Der Administrator kann die Unterstützung des dynamischen Modus für VDI (s. Abschnitt "Dynamischen VDI-Modus in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren" auf S. 219) in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren, der auf der temporären virtuellen Maschine installiert wird.

Wird die temporäre virtuelle Maschine heruntergefahren, informiert der Administrationsagent darüber den Administrationsserver. Wurde die virtuelle Maschine erfolgreich heruntergefahren, wird sie aus der Liste der Geräte entfernt, die mit dem Administrationsserver verbunden sind. Wurde die virtuelle Maschine fehlerhaft heruntergefahren, und der Administrationsagent hat keine Benachrichtigung darüber an den Server gesendet, wird eine Doppel-Vorgehensweise eingesetzt. In diesem Fall wird die virtuelle Maschine nach drei fehlgeschlagenen Synchronisierungsversuchen mit dem Server aus der Liste der mit dem Administrationsserver verbundenen Geräte entfernt.

In diesem Abschnitt

Dynamischen VDI-Modus in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren

Gehen Sie wie folgt vor, um den dynamischen VDI-Modus zu aktivieren:

1. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** den Unterordner **Installationspakete** aus.
2. Klicken Sie mit der rechten Maustaste auf das Installationspaket des Administrationsagenten und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: Kaspersky Security Center Administrationsagent** wird geöffnet.
3. Klicken Sie im Fenster **Eigenschaften: Kaspersky Security Center Administrationsagent** auf den Abschnitt **Erweitert**.
4. Aktivieren Sie im Abschnitt **Erweitert** das Kontrollkästchen **Dynamischen Modus für VDI aktivieren**.

Das Gerät, auf dem der Administrationsagent installiert wird, wird in die Virtual Desktop Infrastructure aufgenommen.

Geräte suchen, die zu VDI gehören

Gehen Sie wie folgt vor, um Geräte zu finden, die zu VDI gehören:

1. Klicken Sie mit der rechten Maustaste auf den Ordner **Nicht zugeordnete Geräte** und wählen Sie **Suchen** aus.

2. Wählen Sie im Fenster **Suchen** auf der Registerkarte **Virtuelle Maschinen** in der Dropdown-Liste **Gehört zur Virtual-Desktop-Infrastruktur (VDI)** die Variante **Ja** aus.

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

Es werden Geräte gesucht, die zur Virtual Desktop Infrastructure gehören.

Geräte, die zu VDI gehören, in eine Administrationsgruppe verschieben

Gehen Sie wie folgt vor, um Geräte, die zur VDI gehören, in eine Administrationsgruppe zu verschieben:

1. Klicken Sie im Arbeitsplatz des Ordners **Nicht zugeordnete Geräte** auf die Schaltfläche **Regeln anpassen**.

   Daraufhin wird das Eigenschaftenfenster des Ordners **Nicht zugeordnete Geräte** geöffnet.

2. Klicken Sie im Eigenschaftenfenster des Ordners **Nicht zugeordnete Geräte** im Abschnitt **Geräte verschieben** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Neue Regel** wird geöffnet.

3. Klicken Sie im Fenster **Neue Regel** auf den Abschnitt **Virtuelle Maschinen**.

4. Wählen Sie in der Dropdown-Liste **Gehört zur Virtual-Desktop-Infrastruktur (VDI)** die Variante **Ja** aus.

Daraufhin wird eine Regel für das Verschieben von Geräten in eine Administrationsgruppe erstellt.

Programmverwaltung auf Client-Geräten

Kaspersky Security Center ermöglicht die Verwaltung von Kaspersky Lab-Programmen und Programmen anderer Hersteller, die auf Client-Geräten installiert sind.

Der Administrator kann folgende Aktionen ausführen:

- Programmkategorien anhand angegebener Kriterien erstellen
- Programmkategorien mithilfe von speziell erstellten Regeln verwalten
- Programmstart auf den Geräten verwalten
- Inventarisierung durchführen und die Programm-Registry für die auf Geräten installierten Programme führen
- Schwachstellen der Programme schließen, die auf Geräten installiert wurden
- Windows-Updates und Updates anderer Softwarehersteller auf Geräten installieren
- Verwendung von Schlüsseln für lizenzierte Programmgruppen verfolgen.

In diesem Abschnitt

Programmgruppen

In diesem Abschnitt werden Vorgänge beschrieben, die für Gruppen von auf Geräten installierten Programmen vorgesehen sind.

Programmkategorien erstellen

Kaspersky Security Center ermöglicht das Erstellen von Programmkategorien der auf den Geräten installierten Programme.

Programmkategorien können auf eine der folgenden Weise erstellt werden:

- Der Administrator gibt einen Ordner an, dessen ausführbaren Dateien in die gewählte Kategorie aufgenommen werden.
- Der Administrator gibt ein Gerät an, dessen ausführbaren Dateien in die gewählte Kategorie aufgenommen werden.
- Der Administrator gibt Kriterien an, nach denen Programme in die gewählte Kategorie aufgenommen werden.

Wenn eine Programmkategorie erstellt wurde, kann der Administrator für diese Kategorie Regeln festlegen. Die Regeln legen das Verhalten der Programme fest, die zur gewählten Kategorie gehören. Der Start von Programmen, die zu dieser Kategorie gehören, kann beispielsweise verboten oder erlaubt sein.

Programmstart auf den Geräten verwalten

Mit Kaspersky Security Center können Sie den Programmstart auf Client-Geräten im Modus "Weiße Liste" verwalten (weitere Details siehe: Administratorhandbuch für das Programm Kaspersky Endpoint Security 10 für Windows). Im Modus "Weiße Liste" können auf den festgelegten Geräten nur solche Programme gestartet werden, die zu den angegebenen Kategorien gehören. Der Administrator kann sich Ergebnisse der statischen Analyse der Regeln für den Programmstart auf Geräten nach jedem Benutzer anzeigen lassen.

Inventarisierung von auf Geräten installierten Programmen

Kaspersky Security Center ermöglicht es, eine Inventarisierung der auf den Geräten installierten Programme durchzuführen. Der Administrationsagent empfängt Informationen über alle Programme, die auf den Geräten installiert wurden. Die bei der Inventarisierung gesammelten Daten werden im Arbeitsplatz des Ordners **Programm-Registry** angezeigt. Der Administrator kann sich ausführliche Informationen zu jedem Programm, einschließlich Version und Hersteller, anzeigen lassen.

Die Anzahl ausführbarer Dateien, die von einem Gerät erhalten werden, darf 150 000 nicht überschreiten. Wenn diese Grenze erreicht wird, erhält Kaspersky Security Center keine neuen Dateien mehr.

Lizenzierte Programmgruppen verwalten

Kaspersky Security Center ermöglicht das Erstellen von lizenzierten Programmgruppen. Zur Gruppe von lizenzierten Programmen gehören Programme, die die vom Administrator festgelegten Kriterien erfüllen. Der Administrator kann folgende Kriterien für lizenzierte Programmgruppen angeben:

- Programmname
- Programmversion
- Hersteller
- Programm-Tag.

Programme, die einem oder mehreren Kriterien entsprechen, werden automatisch in die Gruppe aufgenommen. Um eine Gruppe von lizenzierten Programmen zu erstellen, muss mindestens ein Kriterium für die Aufnahme von Programmen in diese Gruppe angegeben werden.

Jede lizenzierte Programmgruppe hat einen eigenen Schlüssel. Der Schlüssel einer lizenzierten Programmgruppe legt fest, wie viele Installationen für die Programme der Gruppe erlaubt sind. Hat die Anzahl von Installationen die im Schlüssel vorgesehene Einschränkung überschritten, wird auf dem Administrationsserver ein Informationsereignis registriert. Der Administrator kann das Ablaufdatum für den Schlüssel angeben. An diesem Datum wird auf dem Administrationsserver ein Informationsereignis registriert.

Informationen über ausführbare Dateien anzeigen

Kaspersky Security Center empfängt alle Informationen zu ausführbaren Dateien, die seit der Installation des Betriebssystems auf den Geräten gestartet wurden. Die gesammelten Informationen zu ausführbaren Dateien werden im Programmhauptfenster im Arbeitsplatz des Ordners **Ausführbare Dateien** angezeigt.

In diesem Abschnitt

Programmkategorien erstellen

Um eine Programmkategorie zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Programmkategorien** aus.
2. Klicken Sie auf den Link **Kategorie erstellen**, um den Assistenten für das Erstellen von Benutzerkategorien zu starten.
3. Wählen Sie im Fenster des Assistenten den erforderlichen Typ der Benutzerkategorie aus:

- **Manuell zu erweiternde Kategorie**. In diesem Fall können Sie Kriterien manuell angeben, nach denen ausführbare Dateien in die erstellte Kategorie aufgenommen werden sollen.

- **Automatisch zu erweiternde Kategorie**. In diesem Fall können Sie einen Ordner angeben. Die in diesem Ordner befindlichen ausführbaren Dateien werden automatisch in die erstellte Kategorie aufgenommen.

> Beim Erstellen der automatisch ergänzten Kategorie führt das Programm die Inventarisierung folgender Dateiformate aus: exe, com, dll, sys, bat, ps1, cmd, js, vbs, reg, msi, msc, cpl, html, htm, drv, ocx, scr.

- **Kategorie für ausführbare Dateien der gewählten Geräte** In diesem Fall können Sie das Gerät festlegen. Die auf dem Gerät gefundenen ausführbaren Dateien werden automatisch der Kategorie zugeordnet.

4. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird eine benutzerdefinierte Programmkategorie erstellt. Die erstellten Kategorien können in der Kategorieliste im Arbeitsplatz des Ordners **Programmkategorien** angezeigt werden.

Verwaltung des Programmstarts auf Client-Geräten anpassen

Um die Verwaltung des Programmstarts auf Client-Geräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Programmkategorien** aus.

2. Erstellen Sie im Arbeitsbereich des Ordners **Programmkategorien** eine Kategorie für Programme (s. Abschnitt "Programmkategorien erstellen" auf S. 224), deren Start Sie verwalten möchten.

3. Klicken Sie im Ordner **Verwaltete Geräte**auf der Registerkarte **Richtlinien** auf den Link **Richtlinie für Kaspersky Endpoint Security erstellen**, um den Assistenten

für das Erstellen einer Richtlinie für das Programm Kaspersky Endpoint Security 10 für Windows zu starten, und folgen Sie den Anweisungen des Assistenten.

Ist diese Richtlinie bereits vorhanden, können Sie diesen Schritt überspringen. Die Verwaltung des Starts von Programmen der gewählten Kategorie können Sie in den Einstellungen dieser Richtlinie anpassen. Die erstellte Richtlinie wird im Ordner **Verwaltete Geräte** auf der Registerkarte **Richtlinien** angezeigt.

4. Klicken Sie mit der rechten Maustaste auf die Richtlinie für das Programm Kaspersky Endpoint Security 10 für Windows und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Richtlinie für Kaspersky Endpoint Security 10 für Windows geöffnet.

5. Klicken Sie im Eigenschaftenfenster der Richtlinie für Kaspersky Endpoint Security 10 für Windows im Abschnitt **Kontrolle des Programmstarts** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Kontrollregel für den Start von Programmen** wird geöffnet.

6. Wählen Sie im Fenster **Kontrollregel für den Start von Programmen** in der Dropdown-Liste **Kategorie** die Programmkategorie aus, für welche die Regel gelten soll. Passen Sie die Einstellungen der Regel für den Start von Programmen der gewählten Programmkategorien an.

   Ausführliche Informationen über die Kontrollregeln für den Start von Programmen können Sie dem Administratorhandbuch für Kaspersky Endpoint Security 10 für Windows entnehmen.

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

Die Programme, die zur angegebenen Kategorie gehören, werden auf den Geräten nach der angegebenen Regel gestartet. Die erstellte Regel wird im Eigenschaftenfenster der Richtlinie für Kaspersky Endpoint Security 10 für Windows im Abschnitt **Kontrolle des Programmstarts** angezeigt.

Ergebnisse der statischen Analyse der Regeln für den Start ausführbarer Dateien anzeigen

Gehen Sie wie folgt vor, um sich Informationen darüber anzeigen zu lassen, welche ausführbaren Dateien für den Start von Benutzern nicht zugelassen sind:

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** die Registerkarte **Richtlinien**.

2. Klicken Sie mit der rechten Maustaste auf die **Schutzrichtlinie**, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Schutzrichtlinie geöffnet.

3. Klicken Sie im Eigenschaftenfenster der Schutzrichtlinie auf den Abschnitt **Kontrolle des Programmstarts** und anschließend auf die Schaltfläche **Statische Analyse**.

   Das Fenster **Analyse der Liste der Zugriffsrechte**.

4. Im linken Fensterbereich **Analyse der Liste der Zugriffsrechte** wird die Benutzerliste angezeigt, die anhand der Active Directory-Daten erstellt wurde.

5. Wählen Sie in der Liste einen Benutzer aus.

   Im rechten Fensterbereich werden Programmkategorien angezeigt, die diesem Benutzer zugewiesen wurden.

6. Um sich ausführbare Dateien anzeigen zu lassen, deren Start für den Benutzer verboten ist, klicken Sie im Fenster **Analyse der Liste der Zugriffsrechte** auf die Schaltfläche **Dateien anzeigen**.

   Daraufhin wird das Fenster geöffnet, in dem die Liste der ausführbaren Dateien angezeigt wird, deren Start für den Benutzer verboten ist.

7. Um sich die Liste der ausführbaren Dateien anzeigen zu lassen, die zu einer Kategorie gehören, wählen Sie die gewünschte Programmkategorie aus, und klicken Sie auf die Schaltfläche **Kategoriedateien anzeigen**.

Daraufhin wird das Fenster geöffnet, in dem die Liste der ausführbaren Dateien angezeigt wird, die zur gewählten Programmkategorie gehören.

Programm-Registry anzeigen

Das Feature Datensammlung zu installierten Programmen wird nur für Microsoft-Windows-Betriebssysteme unterstützt.

Um sich die Registry der auf den Client-Geräten installierten Programme anzeigen zu lassen,

wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Programm-Registry** aus.

Daraufhin wird im Arbeitsplatz des Ordners **Programm-Registry** die Liste der Programme angezeigt, die der Administrationsagent auf den Geräten gefunden hat, auf denen er installiert ist.

Detaillierte Informationen über ein bestimmtes Programm aus der Liste können Sie über den Punkt **Eigenschaften** im Kontextmenü dieses Programms anzeigen lassen.
Im Eigenschaftenfenster des Programms werden allgemeine Informationen zum Programm und dessen ausführbaren Dateien sowie die Liste der Geräte angezeigt, auf denen das Programm installiert wurde.

Um sich Programme anzeigen zu lassen, die bestimmten Kriterien entsprechen, können Sie die Filterfelder im Arbeitsplatz des Ordners **Programm-Registry** verwenden.

Die Daten zu Programmen von Kaspersky Lab und anderen Herstellern auf den Geräten, die mit untergeordneten und virtuellen Administrationsservern verbunden sind, werden auch in der Programm-Registry des Hauptadministrationsservers gespeichert. Diese Informationen können mithilfe des Berichts über die Programm-Registry eingesehen werden, indem Daten von den untergeordneten und virtuellen Administrationsservern in den Bericht aufgenommen werden.

Um Informationen von untergeordneten Administrationsservern in den Bericht über die Programm-Registry einzuschließen, 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 **Berichte** aus.

3. Wählen Sie im Arbeitsplatz der Registerkarte **Berichte** die Option **Bericht über die Versionen der Kaspersky-Lab-Programme** aus.

4. Klicken Sie mit der rechten Maustaste auf den Bericht und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: Bericht über Versionen der Kaspersky-Lab-Programme** wird geöffnet.

5. Aktivieren Sie im Abschnitt **Hierarchie der Administrationsserver** das Kontrollkästchen **Daten der untergeordneten und virtuellen Administrationsserver einschließen**.

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

Daraufhin werden Informationen über die untergeordneten und virtuellen Administrationsserver in den Bericht **Bericht über die Versionen der Kaspersky-Lab-Programme** aufgenommen.

Lizenzierte Programmgruppen erstellen

Um eine Gruppe von lizenzierten Programmen zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzverwaltung für Drittanbieter-Software** aus.

2. Klicken Sie auf den Link **Lizenzierte Programmgruppe hinzufügen**, um den **Assistent für das Hinzufügen einer lizenzierten Programmgruppe** zu starten.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird eine lizenzierte Programmgruppe erstellt, die im Ordner **Lizenzverwaltung für Drittanbieter-Software** angezeigt wird.

Schlüsselverwaltung für lizenzierte Programmgruppen

Um einen Schlüssel für eine lizenzierte Programmgruppe anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzverwaltung für Drittanbieter-Software** aus.

2. Klicken Sie im Arbeitsplatz des Ordners **Lizenzverwaltung für Drittanbieter-Software** auf den Link **Schlüssel für lizenzierte Programme verwalten**, um das Fenster **Schlüssel für lizenzierte Programme verwalten** zu öffnen.

3. Klicken Sie im Fenster **Schlüssel für lizenzierte Programme verwalten** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Schlüssel** wird geöffnet.

4. Geben Sie im Fenster **Schlüssel** die Einstellungen des Schlüssels und die Einschränkungen an, die bei der Anwendung des Schlüssels für eine lizenzierte Programmgruppe gelten sollen.

   - **Name**. Schlüsselname.

   - **Kommentar**. Anmerkungen zum gewählten Schlüssel.

- **Beschränkung**. Anzahl von Geräten, auf denen das Programm installiert werden kann, das den betreffenden Schlüssel verwendet.

- **Ablaufdatum**. Datum, an dem die Gültigkeitsdauer des Schlüssels endet.

Die angelegten Schlüssel werden im Fenster **Schlüssel für lizenzierte Programme verwalten** angezeigt.

Gehen Sie wie folgt vor, um einen Schlüssel auf eine lizenzierte Programmgruppe anzuwenden:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzverwaltung für Drittanbieter-Software** aus.

2. Wählen Sie im Ordner **Lizenzverwaltung für Drittanbieter-Software** die lizenzierte Programmgruppe aus, auf die Sie den Schlüssel anwenden möchten.

3. Klicken Sie mit der rechten Maustaste auf die Gruppe von lizenzierten Programmen und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Gruppe von lizenzierten Programmen geöffnet.

4. Wählen Sie im Eigenschaftenfenster der Gruppe von lizenzierten Programmen im Abschnitt **Schlüssel** die Option **Verstoß gegen die festgelegten Lizenzbeschränkungen protokollieren** aus.

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

   Das Fenster **Schlüssel auswählen** wird geöffnet.

6. Wählen Sie im Fenster **Schlüssel auswählen** den Schlüssel aus, den Sie auf die Gruppe von lizenzierten Programmen anwenden möchten.

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

Die im Schlüssel vorgesehenen Einschränkungen für eine Gruppe von lizenzierten Programmen werden auf die gewählte Gruppe verteilt.

Software von Kaspersky Security Center inventarisieren

Kaspersky Security Center führt eine Inventarisierung der Software durch, die auf den verwalteten Client-Geräten installiert ist.

Der Administrationsagent erstellt eine Liste der auf dem Gerät installierten Programme und leitet die Liste an den Administrationsserver weiter. Der Administrationsagent erhält Informationen über die installierten Programme automatisch aus der Windows-Registry.

Um die Ressourcen des Geräts zu speichern beginnt der Administrationsagent standardmäßig 10 Minuten nach dem Start des Dienstes des Administrationsagenten, Informationen über die installierten Programme abzurufen.

Um die Zeitspanne für den Beginn der Softwareinventarisierung des Geräts nach dem Start des Dienstes des Administrationsagenten zu ändern, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Systemregistrierung des Geräts, auf dem der Administrationsagent 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\1103\1.0.0.0\NagentFlags

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags

3. Legen Sie für den Schlüssel KLINV_INV_COLLECTOR_START_DELAY_SEC den gewünschten Wert in Sekunden fest.

   Standardmäßig ist der Wert auf 600 Sekunden eingestellt.

4. Starten Sie den Dienst des Administrationsagenten neu.

Daraufhin wird die Zeitspanne für den Beginn der Softwareinventarisierung nach dem Start des Dienstes des Administrationsagenten geändert.

Inventarisierung der ausführbaren Dateien

Die Inventarisierung der ausführbaren Dateien auf den Client-Geräten kann mithilfe von Inventarisierungsaufgaben ausgeführt werden. Die Inventarisierungsfunktion für ausführbare Dateien ist im Programm Kaspersky Endpoint Security 10 für Windows implementiert.

Die Anzahl ausführbarer Dateien, die von einem Gerät erhalten werden, darf 150 000 nicht überschreiten. Wenn diese Grenze erreicht wird, erhält Kaspersky Security Center keine neuen Dateien mehr.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wahlen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Klicken Sie im Arbeitsplatz des Ordners **Aufgaben** auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet.

3. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Kaspersky Endpoint Security** und den Aufgabenuntertyp **Inventarisierung**. Klicken Sie dann auf die Schaltfläche **Weiter**.
4. Folgen Sie den weiteren Schritten des Assistenten.

Nach der Ausführung des Assistenten wird eine Inventarisierungsaufgabe für Kaspersky Endpoint Security erstellt. Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsplatz des Ordners **Aufgaben** angezeigt.

Eine Liste der auf den Geräten als Ergebnis der Ausführung der Inventarisierungsaufgaben gefundenen ausführbaren Dateien wird im Arbeitsplatz des Ordners **Ausführbare Dateien** angezeigt.

Während der Inventarisierung findet das Programm ausführbare Dateien folgender Formate: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, sowie HTML-Dateien.

Informationen über ausführbare Dateien anzeigen

Um sich die Liste aller auf den Client-Geräten gefundenen ausführbaren Dateien anzeigen zu lassen,

Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Ausführbare Dateien** aus.

Im Arbeitsplatz des Ordners **Ausführbare Dateien** wird die Liste der ausführbaren Dateien angezeigt, die auf den Geräten seit der Installation des Betriebssystems ausgeführt oder während der Ausführung der Inventarisierungsaufgabe von Kaspersky Endpoint Security 10 für Windows gefunden wurden.

Um sich die Daten zu den ausführbaren Dateien anzeigen zu lassen, die bestimmten Kriterien entsprechen, können Sie den Filter verwenden.

Um sich die Eigenschaften einer ausführbaren Datei anzeigen zu lassen,

klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Fenster geöffnet, in dem Informationen über die ausführbare Datei sowie Geräte angezeigt werden, auf denen die ausführbare Datei vorhanden ist.

Schwachstellen in Programmen

Der Ordner **Schwachstellen in Programmen** innerhalb des Ordners **Programmverwaltung** enthält ein Verzeichnis von Programmschwachstellen, die auf Client-Geräten vom auf ihnen installierten Administrationsagenten gefunden wurden.

> Das Feature Datenanalyse über Schwachstellen in Programmen wird nur für Microsoft-Windows-Betriebssysteme unterstützt.

Durch Öffnen des Eigenschaftsfensters für ein ausgewähltes Programm im Ordner **Schwachstellen in Programmen** erhalten Sie Zugang zu allgemeinen Informationen zur Schwachstelle, zum betroffenen Programm, zur Liste aller Geräte, auf denen Schwachstellen festgestellt wurden sowie zu Hinweisen, wie diese behoben werden können.

Informationen über Schwachstellen in Programmen finden Sie auf der Website von Kaspersky Lab (https://threats.kaspersky.com/).

Informationen über Schwachstellen in Programmen anzeigen

Um sich die Liste der Schwachstellen anzeigen zu lassen, die auf den Client-Geräten gefunden wurden,

wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

Im Arbeitsplatz des Ordners wird die Liste von Schwachstellen in Programmen angezeigt, die der auf den Client-Geräten installierte Administrationsagent gefunden hat.

Um Informationen über eine gewählte Schwachstelle abzufragen,

klicken Sie mit der rechten Maustaste auf die Schwachstelle und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Eigenschaftenfenster der Schwachstelle geöffnet, in dem folgende Informationen angezeigt werden:

- Programm, in dem die Schwachstelle gefunden wurde
- Liste der Geräte, auf denen die Schwachstelle gefunden wurde
- Informationen zum Schließen der Schwachstelle.

Um sich einen Bericht über alle gefundenen Schwachstellen anzeigen zu lassen,

klicken Sie im Ordner **Schwachstellen in Programmen** auf den Link **Bericht über Schwachstellen in Programmen anzeigen**.

Daraufhin wird ein Bericht über Schwachstellen in Programmen erstellt, die auf den Geräten vorhanden sind. Der Bericht kann im Knoten mit dem Namen des gewünschten Administrationsservers auf der Registerkarte "Berichte" angezeigt werden.

Das Feature Datensammlung über Schwachstellen in Programmen wird nur für Microsoft-Windows-Betriebssysteme unterstützt.

Schwachstellensuche in Programmen

Wenn Sie das Programm mit dem Schnellstartassistenten konfiguriert haben, wird die Aufgabe zur Schwachstellensuche automatisch angelegt. Die Aufgabe kann im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** angezeigt werden.

Gehen Sie wie folgt vor, um eine Aufgabe zur Schwachstellensuche in den auf Client-Geräten installierten Programmen anzulegen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

2. Klicken Sie im Arbeitsplatz auf den Link **Suche nach Schwachstellen anpassen**, um den Assistenten für das Erstellen einer Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates zu starten.

   Das Fenster des Assistenten für das Erstellen von Aufgaben wird geöffnet.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe **Nach Schwachstellen und erforderlichen Updates suchen** erstellt, die in der Aufgabenliste im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** angezeigt wird.

Nach der Ausführung der Aufgabe **Nach Schwachstellen und erforderlichen Updates suchen** werden auf dem Administrationsserver eine Liste mit gefundenen Schwachstellen in der auf dem Gerät installierten Software sowie die notwendigen Software-Updates für die Geräte im Netzwerk (z. B. neue Programmversionen) angezeigt.

Der Administrationsagent erhält Informationen über verfügbare Updates für Windows und andere Microsoft-Software vom Dienst Windows Update-Agent oder vom Administrationsserver, falls dieser als WSUS-Server verwendet wird. Die Informationen werden zum Zeitpunkt des Programmstarts (falls in der Richtlinie festgelegt) und beim regelmäßigen Start der Aufgabe **Windows-Updates synchronisieren** auf den Client-Geräten übergeben.

Informationen zu Drittanbietersoftware, die mithilfe von Kaspersky Security Center aktualisiert werden kann, finden Sie auf der Website des Technischen Supports, auf der Seite von Kaspersky Security Center im Abschnitt Server-Verwaltung (http://support.kaspersky.com/de/9327).

Schwachstellen in Programmen schließen

Wenn Sie im Schnellstartassistenten im Fenster **Einstellungen für die Verwaltung von Updates** die Option **Erforderliche Updates für Programme suchen und installieren** ausgewählt haben, wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** automatisch erstellt. Die Aufgabe wird im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** angezeigt.

Gehen Sie wie folgt vor, um eine Aufgabe zum Schließen von Schwachstellen mit verfügbaren Updates für Programme anzulegen:

1. Wählen Sie in der Konsolenstruktur auf der Registerkarte **Aufgaben** den Ordner **Verwaltete Geräte** aus.

2. Klicken Sie auf den Link **Aufgabe erstellen**, um den Assistenten für das Erstellen von Aufgaben zu starten.

3. Geben Sie im Fenster des Assistenten **Aufgabentyp auswählen** den Aufgabentyp **Erforderliche Updates installieren und Schwachstellen schließen** an.

4. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** erstellt, die im Ordner **Aufgaben** angezeigt wird.

Um die ausgewählte Schwachstelle mithilfe von verfügbaren Updates für Programme zu schließen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Schwachstellen in Programmen** aus.

2. Klicken Sie im Ordner **Software-Updates** auf die Schaltfläche **Assistent zum Schließen von Schwachstellen starten**.

   Der Assistent zum Schließen von Schwachstellen wird geöffnet.

   > Das Funktional des Assistenten zum Schließen von Schwachstellen starten ist aktiv, wenn eine Lizenz für die Funktion Systems Management vorhanden ist.

3. Folgen Sie den Anweisungen des Assistenten.

Während der Ausführung des Assistenten wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** erstellt und im Ordner **Aufgaben** angezeigt. Alternativ wird eine Regel zum Schließen von Schwachstellen zur existierenden Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** hinzugefügt.

Software-Updates

Kaspersky Security Center ermöglicht die Verwaltung von Software-Updates für auf Client-Geräten installierte Programme und das Schließen von Schwachstellen in Programmen von Microsoft und anderen Softwareherstellern durch die Installation erforderlicher Updates.

Kaspersky Security Center führt die Suche nach Updates mit der Aufgabe zur Suche nach Updates durch und lädt die Updates in die Update-Datenverwaltung herunter. Nach Abschluss der Update-Suche stellt das Programm dem Administrator die Informationen über die verfügbaren Updates und die Programmschwachstellen bereit, die mit diesen Updates geschlossen werden können.

Die Informationen über die verfügbaren Microsoft Windows-Updates werden vom Windows Update Center übertragen. Der Administrationsserver kann die Rolle des Windows Update-Servers übernehmen (WSUS). Um den Administrationsserver als Windows Update-Server zu verwenden, ist es erforderlich, die Synchronisierung von Updates mit dem Windows Update Center einzustellen. Sobald die Synchronisierung der Daten mit dem Windows Update Center eingerichtet wurde, stellt der Administrationsserver im angegebenen Intervall Updates für die Windows Update-Dienste auf den Geräten bereit.

Außerdem können Software-Updates mit der Richtlinie des Administrationsagenten verwaltet werden. Dazu ist es erforderlich, eine Richtlinie für den Administrationsagenten zu erstellen und die Einstellungen für Software-Updates in den betreffenden Fenstern des Assistenten für das Erstellen der Richtlinie anzupassen.

Der Administrator kann sich die Liste der verfügbaren Updates im Ordner **Software-Updates** anzeigen lassen, der zum Ordner **Programmverwaltung** gehört. Dieser Ordner enthält eine Liste der durch den Administrationsserver heruntergeladenen Updates für Microsoft-Programme und Programme anderer Softwarehersteller, die auf Geräte verteilt werden können. Nachdem Durchsicht der Informationen über die verfügbaren Updates kann der Administrator die Installation von Updates auf den Geräten durchführen.

Das Update einiger Programme von Kaspersky Security Center wird mittels Deinstallation der vorherigen Programmversion und Installation der neuen Version durchgeführt.

Vor der Installation von Updates auf allen Geräten können Sie eine Probeinstallation durchführen, um sich zu vergewissern, dass die installierten Updates zu keinen Störungen der Programme auf den Geräten führen.

Informationen zu Drittanbietersoftware, die mithilfe von Kaspersky Security Center aktualisiert werden kann, finden Sie auf der Website des Technischen Supports, auf der Seite von Kaspersky Security Center im Abschnitt Server-Verwaltung (http://support.kaspersky.com/de/9327).

In diesem Abschnitt

Informationen über verfügbare Updates anzeigen

Um sich eine Liste der verfügbaren Updates für die auf den Client-Geräten installierten Programme anzeigen zu lassen,

Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Software-Updates** aus.

Im Arbeitsplatz des Ordners können Sie sich die Liste der vorhandenen Updates für die auf den Geräten installierten Programme anzeigen lassen.

Um sich die Eigenschaften eines Updates anzeigen zu lassen,

klicken Sie mit der rechten Maustaste auf das erforderliche Update im Arbeitsplatz des Ordners **Software-Updates** und wählen Sie den Punkt **Eigenschaften** aus.

Im Eigenschaftenfenster des Updates werden folgende Informationen angezeigt:

- Liste der Client-Geräte, für die das Update anwendbar ist (*Zielgeräte*);
- Liste der systemweiten Komponenten (Voraussetzungen), die vor der Installation von Updates installiert werden müssen (wenn solche Komponenten vorhanden sind);
- Schwachstellen in Programmen, die durch dieses Update geschlossen werden.

Windows-Updates mit dem Administrationsserver synchronisieren

Haben Sie im Schnellstartassistenten im Fenster **Einstellungen für die Verwaltung von Updates** die Option **Administrationsserver als WSUS-Server verwenden** ausgewählt, wird die Aufgabe zur Synchronisierung von Windows-Updates automatisch erstellt. Sie können die Aufgabe im Ordner **Aufgaben** starten. Die Funktion der Microsoft Software-Updates ist erst nach einem erfolgreichen Abschluss der Aufgabe **Windows-Updates synchronisieren** verfügbar.

Gehen Sie wie folgt vor, um die Aufgabe zur Synchronisierung von Windows-Updates mit dem Administrationsserver anzulegen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Software-Updates** aus.

2. Klicken Sie auf die Schaltfläche **Erweiterte Aktionen** und wählen Sie in der Dropdown-Liste den Punkt **Synchronisierung von Windows-Updates anpassen**.

   Daraufhin wird der Assistent für das Erstellen einer Aufgabe zum Abrufen von Daten aus dem Windows Update Center gestartet.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe **Windows-Updates synchronisieren** angelegt, die im Ordner **Aufgaben** angezeigt wird.

> Sie können eine Aufgabe zur Synchronisierung von Windows-Updates auch mit dem Link **Aufgabe erstellen** im Ordner **Aufgaben** anlegen.

Die Aufgabe **Windows-Updates synchronisieren** lädt nur Metadaten von den Microsoft-Servern herunter. Wenn im Netzwerk kein WSUS-Server verwendet wird (wenn also jedes Client-Gerät die Microsoft-Updates selbständig von externen Servern herunterlädt).

Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren

Sie können das automatische Datenbanken-Update und das Update der Programm-Module von Kaspersky Endpoint Security auf den Client-Geräten konfigurieren.

Um den Download und die automatische Installation von Updates für Kaspersky Endpoint Security auf den Geräten anzupassen, gehen Sie wie folgt vor:

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

2. Erstellen Sie eine Aufgabe mit dem Typ **Update** auf eine der folgenden Weisen:

   - Wählen Sie im Kontextmenü des Ordners **Aufgaben** der Konsolenstruktur den Punkt **Erstellen** → **Aufgabe** aus.

- Klicken Sie im Arbeitsplatz des Ordners **Aufgaben** auf die Schaltfläche **Aufgabe erstellen**.

Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet.

3. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Kaspersky Endpoint Security** und den Aufgabenuntertyp **Update**. Klicken Sie dann auf die Schaltfläche **Weiter**.

4. Folgen Sie den weiteren Schritten des Assistenten.

   Nach der Ausführung des Assistenten wird eine Update-Aufgabe für Kaspersky Endpoint Security erstellt. Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsplatz des Ordners **Aufgaben** angezeigt.

5. Wählen Sie im Arbeitsplatz des Ordners **Aufgaben** die erstellte Update-Aufgabe aus.

6. Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

7. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.

   Im Abschnitt **Einstellungen** können Sie die Einstellungen für die Update-Aufgabe im lokalen und autonomen Modus anpassen:

   - **Update-Einstellungen im lokalen Modus**: zwischen dem Gerät und Administrationsserver ist eine Verbindung hergestellt.

   - **Update-Einstellungen im autonomen Modus**: zwischen dem Gerät und Kaspersky Security Center besteht keine Verbindung (wenn beispielsweise das Gerät nicht mit dem Internet verbunden ist).

8. Mithilfe der Schaltfläche **Einstellungen** wählen Sie die Update-Quelle.

9. Aktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen**, um die Updates für die Programm-Module einmalig von den Programm-Datenbanken herunterzuladen und zu installieren.

   Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Endpoint Security den Benutzer über verfügbare Updates für Programm-Module und aktiviert während

der Ausführung der Update-Aufgabe das Update der Programm-Module im Update-Paket. Passen Sie das Übernehmen der Updates durch die Module an:

- **Kritische und genehmigte Updates installieren**. Wenn Updates für die Programm-Module verfügbar sind, installiert Kaspersky Endpoint Security Updates mit dem Status *Kritisch* automatisch, und die restlichen Updates der Programm-Module nach Installationsfreigabe durch den Administrator.

  Gehen Sie folgendermaßen vor, um Software-Updates freizugeben:

  a. Öffnen Sie in der Konsolenstruktur den Ordner **Software-Updates**.

  b. Legen Sie im Eigenschaftenfenster des Updates im Abschnitt **Allgemein** im Feld **Updates genehmigen** den Wert **Genehmigt** fest.

  Als Standard gilt der Wert **Nicht festgestellt**.

  > Wenn Sie bei der Konfiguration des Updates für Kaspersky-Lab-Programme, die nicht deinstalliert werden können, im Feld **Updates genehmigen** den Wert **Deaktiviert** angeben, wird Kaspersky Security Center ein solches Update nicht von Geräten deinstallieren, auf denen es zuvor installiert wurde.
  >
  > Im Eigenschaftenfenster des Updates auf der Registerkarte **Allgemein** im Feld **Anforderungen bei der Installation** wird angezeigt, dass das Update für Kaspersky-Lab-Programme nicht deinstalliert werden kann.

- **Nur bestätigte Updates installieren**. Verfügbare Updates für Programm-Module von Kaspersky Endpoint Security werden installiert, nachdem die Installation entweder lokal über die Benutzeroberfläche des Programms oder über Kaspersky Security Center genehmigt wurde.

Wenn für es für das Update von Programm-Modulen erforderlich ist, dass sich der Benutzer mit dem Bedingungen des Lizenzvertrags vertraut macht und diese akzeptiert, werden die Updates installiert, nachdem der Benutzer die Bedingungen des Lizenzvertrags akzeptiert hat.

10. Aktivieren Sie das Kontrollkästchen **Updates in Ordner kopieren**, damit das Programm die heruntergeladenen Updates in den mithilfe der Schaltfläche **Durchsuchen** ausgewählten Ordner kopiert.

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

Beim Ausführen der Aufgabe **Update** sendet das Programm Anfragen an die Kaspersky-Lab-Update-Server.

Einige Updates erfordern die Installation aktueller Plug-In-Versionen für die verwalteten Programme.

Offline-Modell für den Download von Updates

Die Administrationsagenten auf den verwalteten Geräten können nicht immer eine Verbindung zum Administrationsserver herstellen, um Updates herunterzuladen. Ein Administrationsagent kann beispielsweise auf einem Notebook installiert sein, das manchmal nicht mit dem Internet oder dem lokalen Netzwerk verbunden ist. Außerdem kann der Administrator die Verbindungszeit der Geräte mit dem Netzwerk beschränken. In solchen Fällen können die Administrationsagenten Updates vom Administrationsserver nicht nach Zeitplan herunterladen. Wenn ein Update eines verwalteten Programms (beispielsweise Kaspersky Endpoint Security) mithilfe eines Administrationsagenten konfiguriert ist, ist für das Update eine Verbindung zum Administrationsserver erforderlich. Kommt keine Verbindung zwischen Administrationsagent und Administrationsserver zustande, ist kein Update möglich. Die Verbindung zwischen Administrationsagent und Server kann so konfiguriert sein, dass sich der Agent nur zu bestimmten Zeiten mit dem Server verbindet. Im schlechtesten Fall, wenn sich die festgelegten Verbindungsintervalle mit Zeiträumen überschneiden, zu denen keine Verbindung zustande kommt, werden die Datenbanken niemals aktualisiert. Ferner kann es zu Situationen kommen, in denen viele verwaltete Programme gleichzeitig auf den Administrationsserver zugreifen, um Updates herunterzuladen. In einem solchen Fall kann der Administrationsserver die Beantwortung von Anfragen einstellen (wie während eines DDoS-Angriffs).

Zur Vermeidung der aufgeführten Probleme verfügt Kaspersky Security Center über ein Offline-Modell für den Download von Datenbanken-Updates und Modulen der verwalteten Programme. Dieses Modell gewährleistet die Zuverlässigkeit des Mechanismus der Update-Verteilung unabhängig von vorübergehender Unzugänglichkeit der Übertragungskanäle des Administrationsservers und verringert die Auslastung des Administrationsservers.

So funktioniert das Offline-Modell für den Download von Updates

Jedes Mal, wenn der Administrationsserver ein Update erhält, informiert er die Administrationsagenten darüber, welche Updates für die verwalteten Programme erforderlich sind. Sobald die Administrationsagenten die Information erhalten, welche Updates für die verwalteten Programme in Kürze erforderlich sein werden, laden sie die benötigten Dateien vorher vom Administrationsserver herunter. Bei der ersten Verbindung zum Administrationsagenten wird der Download durch diesen Agenten vom Server initiiert. Um die Auslastung auf dem Administrationsserver zu verteilen, beginnen die Administrationsagenten damit, sich während eines vom Server festgelegten Intervalls zufällig mit dem Server zu verbinden und die Updates herunterzuladen. Diese Zeitspanne hängt von der Anzahl von Administrationsagenten, die Updates herunterladen, sowie von der Größe der Updates ab. Nachdem der Administrationsagent alle Updates auf das Gerät heruntergeladen hat, stehen die Updates den Programmen auf dem Gerät zur Verfügung.

Um die Auslastung auf dem Administrationsserver zu verringern, können Sie die Administrationsagenten als Update-Agenten verwenden.

Wenn ein verwaltetes Programm auf dem Gerät auf den Administrationsagenten zugreift, um ein Update herunterzuladen, überprüft der Agent, ob er über das erforderliche Update verfügt. Wurden die Updates erst 25 Stunden vor der Anfrage des verwalteten Programms vom Administrationsserver abgerufen, stellt der Administrationsagent keine Verbindung zum Administrationsserver her, sondern stellt dem verwalteten Programm die Updates aus dem lokalen Cache bereit. In diesem Fall ist keine Verbindung zum Administrationsserver erforderlich und wird für das Update auch nicht benötigt. Im gegenteiligen Fall erfolgt die Installation der Updates im Standardmodus gemäß dem Zeitplan der Aufgabe zum Update-Download.

Das Offline-Modell für den Download von Updates ist standardmäßig aktiviert. Das Offline-Modell für den Download von Updates wird nur für solche verwalteten Geräte verwendet, auf denen der Zeitplan „Nach Beenden der Serveraufgabe zum Update-Download“ für die Aufgaben zum Update-Download durch verwaltete Produkte gilt. Für die übrigen verwalteten Geräte wird das traditionelle System zum Update-Download vom Administrationsserver in Echtzeit verwendet.

Es wird empfohlen, das Offline-Modell für den Download von Updates in den Einstellungen der Richtlinien des Administrationsagenten der entsprechenden Administrationsgruppen zu deaktivieren, wenn laut Konfiguration der verwalteten Produkte der Update-Download nicht vom Administrationsserver, sondern von den Kaspersky-Lab-Servern oder aus einem Netzwerkordner vorgenommen wird, und wenn dabei für die Aufgabe zum Update-Download der Zeitplan "Nach Beenden der Serveraufgabe zum Update-Download" gilt.

Vor- und Nachteile des Offline-Modells für den Download von Updates

Das Offline-Modell für den Download von Updates hat folgende Vorteile:

- Kaspersky Security Center kann selbstständig bestimmen, wann Updates heruntergeladen werden, daher können Update-Fehler der verwalteten Programme verhindert werden. Die Programme haben immer sicheren Zugriff auf die aktuellsten Updates, die vom Administrationsserver heruntergeladen werden können.
- Der Administrationsserver hat die Möglichkeit, die Auslastung bei der Verteilung der Updates zu kontrollieren.

Das Offline-Modell für den Download von Updates hat folgende Nachteile:

- Der Netzwerk-Datenverkehr zwischen Administrationsserver und Administrationsagent kann sich erhöhen, da im Offline-Modell die Updates jedes Mal, nachdem der Administrationsserver neue Updates erhält, auf die Administrationsagenten verteilt werden. Im Standardmodus werden die Updates gemäß dem Zeitplan der Update-Aufgaben verteilt.
- Es kann zu einer zusätzlichen Auslastung auf dem Administrationsserver kommen, weil der Server bestimmen muss, welche Updates jeweils für ein verwaltetes Gerät benötigt werden.

Empfehlungen für die Verwendung des Offline-Models für den Download von Updates

- Es gibt immer eine Zeitspanne zwischen dem Zeitpunkt, zu dem der Administrationsserver neue Updates des Programms erhalten hat, und dem Zeitpunkt, zu dem der Administrationsagent den Download der Updates vom Administrationsserver abgeschlossen hat. Wenn die Update-Aufgabe in diesem Zeitraum beginnt, erhalten die verwalteten Geräte vom Administrationsagenten veraltete Datenbanken-Updates.

  Es wird daher empfohlen, den Zeitplan für die Update-Aufgabe so einzurichten, dass das Update erst dann beginnt, wenn der Administrationsserver alle Updates erhalten hat. In diesem Fall wird die Update-Aufgabe von Kaspersky Security Center ausgeführt, und die Programme erhalten die Updates möglichst rasch.

- Wird die Update-Aufgabe zu früh gestartet, hat der Administrationsagent möglicherweise nicht genügend Zeit, um alle Updates herunterzuladen, bevor die Aufgabe planmäßig gestartet wird.

  Es wird empfohlen, die Zeitspanne zwischen den Starts der Aufgabe für den Download von Updates in den Speicher zu verlängern.

Offline-Modell für den Download von Updates aktivieren und deaktivieren

Um das Offline-Modell zum Abrufen von Updates für die Administrationsgruppe zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur die Administrationsgruppe, für die das Offline-Modell zum Abrufen von Updates aktiviert werden soll.

2. Öffnen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien**.

3. Auf der Registerkarte **Richtlinien** wählen Sie die Richtlinie des Administrationsagenten aus.

4. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Richtlinie des Administrationsagenten geöffnet.

5. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Verwaltung von Patches und Updates**.

6. Installieren Sie oder deaktivieren Sie das Kontrollkästchen**Updates und Antiviren-Datenbanken vom Administrationsserver vorab herunterladen**, um das Offline-Modell zum Abrufen von Updates zu aktivieren oder zu deaktivieren.

   Das Offline-Modell für den Download von Updates ist standardmäßig aktiviert.

Das Offline-Modell für den Download von Updates wird daraufhin aktiviert oder deaktiviert.

Um das Offline-Modell zum Abrufen von Updates gleichzeitig für alle Administrationsgruppen zu aktivieren oder zu deaktivieren, 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\1093\1.0.0.0\ServerFlags

   - Für 32-Bit-Systeme:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Components\34\1093\1.0.0.0\ServerFlags

3. Legen Sie für den Schlüssel SrvDisableOfflineUpdates (DWORD) einen der Werte fest: 0 – um das Offline-Modell zum Abrufen von Updates zu aktivieren; 1 – um das Offline-Modell zum Abrufen von Updates zu deaktivieren.

   Standardmäßig ist für diesen Schlüssel der Wert 0 festgelegt (das Offline-Modell für den Download von Updates ist aktiviert).

4. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird das Offline-Modell zum Abrufen von Updates für alle Administrationsgruppen deaktiviert werden.

Manuelle Installation von Updates auf Geräte

Wenn Sie im Schnellstartassistenten im Fenster **Einstellungen für die Verwaltung von Updates** die Option **Erforderliche Updates für Programme suchen und installieren** ausgewählt haben, wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** automatisch erstellt. Sie können die Aufgabe im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** beenden oder starten.

Wenn Sie im Schnellstartassistenten die Variante **Nach den für die Installation erforderlichen Updates suchen** ausgewählt haben, können Sie Software-Updates mit der Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** auf den Client-Geräten installieren.

Um eine Aufgabe für die Installation von Updates zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Software-Updates** aus.

2. Klicken Sie mit der rechten Maustaste im Ordner **Software-Updates** auf das erforderliche Update und wählen **Update installieren** → **Neue Aufgabe** aus. Oder klicken Sie im Arbeitsbereich mit den markierten Updates auf den Link **Update installieren (Aufgabe erstellen)**.

   Daraufhin wird der Assistent für die Erstellung einer Aufgabe Programm-Updates installieren und Schwachstellen schließen gestartet.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** erstellt, die im Ordner **Aufgaben** angezeigt wird.

In den Einstellungen der Aufgabe für die Update-Installation und das Beheben von Schwachstellen können Sie die automatische Installation systemweiter Komponenten (Voraussetzungen) zulassen, die vor der Installation von Updates installiert werden müssen. In diesem Fall werden vor der Update-Installation alle erforderlichen systemweiten Komponenten installiert. Diese Komponenten sind in den Update-Eigenschaften aufgelistet.

In den Einstellungen der Aufgabe für die Update-Installation und für das Beheben von Schwachstellen können Sie die Installation von Updates zulassen, bei deren Installation eine neue Programmversion installiert wird.

Wenn in den Einstellungen der Aufgabe Regeln für die Installation von Updates von Drittherstellern konfiguriert sind, lädt der Administrationsserver erforderliche Updates von der Website des Herstellers herunter. Die Updates werden in der Datenverwaltung des Administrationsservers gespeichert und auf Geräte, auf denen sie anzuwenden sind, verteilt und installiert.

Wenn in den Einstellungen der Aufgabe Regeln für die Installation von Microsoft-Updates konfiguriert sind und der Administrationsserver als WSUS-Server verwendet wird, lädt der Administrationsserver die notwendigen Updates in die Datenverwaltung und verteilt sie auf die verwalteten Geräte. Wenn im Netzwerk kein WSUS-Server verwendet wird, lädt jedes Client-Gerät die Microsoft-Updates selbständig von externen Servern herunter.

Um eine Aufgabe zur Installation des ausgewählten Updates zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Software-Updates** aus.

2. Klicken Sie im Ordner **Software-Updates** auf die Schaltfläche **Assistent zur Installation von Updates starten**.

   Der Assistent zur Installation von Updates wird geöffnet.

   > Die Funktionen des Update-Assistenten sind bei Vorhandensein der Lizenz für die Funktionalität Systems Management verfügbar.

3. Folgen Sie den Anweisungen des Assistenten.

Während der Ausführung des Assistenten wird die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** erstellt und im Ordner **Aufgaben** angezeigt. Alternativ wird eine neue Regel für die Update-Installation zur existierenden Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** hinzugefügt.

Nach der Installation einer neuen Programmversion kann es in anderen Programmen zu Störungen kommen, die auf Geräten installiert sind und die von dem aktualisierten Programm abhängen.

Sie können die Testinstallation von Updates in den Einstellungen der Aufgabe zur Installation von Updates anpassen.

Gehen Sie wie folgt vor, um die Testinstallation von Updates anzupassen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Verwaltete Geräte** auf der Registerkarte **Aufgaben** die Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** aus.

2. Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Aufgabe **Erforderliche Updates installieren und Schwachstellen schließen** geöffnet.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe im Abschnitt **Testinstallation** eine der Varianten der Testinstallation:

   - **Nicht prüfen**. Wählen Sie diese Option aus, wenn Sie keine Testinstallation von Updates ausführen möchten.

   - **Untersuchung auf angegebenen Geräten ausführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf bestimmten Geräten prüfen möchten. Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie die Geräte aus, auf denen Sie die Testinstallation von Updates ausführen möchten.

   - **Prüfung auf den Geräten in der angegebenen Gruppe durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf einer Gruppe von Geräten prüfen möchten. Geben Sie im Feld **Geben Sie eine Testgruppe an** eine Gruppe von Geräten an, auf denen eine Testinstallation ausgeführt werden soll.

- **Untersuchung für die angegebene Prozentzahl von Geräten ausführen**. Wählen Sie diese Option aus, wenn Sie die Untersuchung der Updates auf einem Teil der Geräte durchführen möchten. Geben Sie im Feld **Prozentanteil der Testgeräte von der gesamten Anzahl von Zielgeräten** den Prozentanteil der Geräte an, auf denen Sie die Testinstallation von Updates ausführen möchten.

4. Geben Sie bei jeder Auswahl, ausgenommen der ersten Variante, im Feld **Zeitraum, in dem ein Entschluss über das Fortsetzen der Installation gefasst werden soll** die Anzahl von Stunden an, die nach der Testinstallation der Updates und vor dem Beginn der Installation der Updates auf allen Geräten vergehen sollen.

Windows-Updates in der Richtlinie des Administrationsagenten anpassen

Um Windows Update in der Richtlinie des Administrationsagenten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Verwaltete Geräte** auf der Registerkarte **Richtlinien** eine Richtlinie des Administrationsagenten aus.

2. Klicken Sie mit der rechten Maustaste auf die Richtlinie, und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster der Richtlinie des Administrationsagenten geöffnet.

3. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Updates und Schwachstellen in Programmen**.

4. Aktivieren Sie das Kontrollkästchen **Administrationsserver als WSUS-Server verwenden**, um Windows-Updates auf den Administrationsserver herunterzuladen und sie dann auf die Client-Geräte mithilfe der Administrationsagenten zu verteilen.

   Wenn das Kontrollkästchen deaktiviert ist, werden die Windows-Updates nicht auf den Administrationsserver heruntergeladen. In diesem Fall erhalten die Client-Geräte die Windows-Updates selbständig.

5. Wählen Sie einen Modus für die Suche von Windows-Updates:

- **Online**. Der Administrationsserver initiiert auf dem Client-Gerät den Zugriff des Windows-Update-Agenten auf die Update-Quelle: Windows Update-Server oder WSUS. Der Administrationsagent überträgt die vom Windows-Update-Agenten abgerufenen Daten an den Administrationsserver.

- **Offline**. In diesem Modus überträgt der Administrationsagent regelmäßig Informationen über Updates, die bei der letzten Synchronisierung des Windows-Update-Agenten mit der Update-Quelle abgerufen wurden, vom Windows-Update-Agenten an den Administrationsserver. Wird die Synchronisierung des Windows-Update-Agenten mit der Update-Quelle nicht ausgeführt, veralten die Daten über Updates auf dem Administrationsserver.

- **Deaktiviert**. Der Administrationsserver erhält keine Informationen über Updates.

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Remote-Installation von Betriebssystemen und Programmen

Kaspersky Security Center ermöglicht das Erstellen und die Verteilung von Betriebssystem-Abbildern auf Client-Geräten eines Netzwerks sowie die Remote-Installation von Kaspersky Lab-Programmen und Programmen anderer Software-Hersteller.

Betriebssystem-Abbilder aufzeichnen

Kaspersky Security Center ermöglicht das Aufzeichnen von Betriebssystem-Abbildern der Zielgeräte und die Übertragung der Abbilder auf den Administrationsserver. Die dadurch erstellten Betriebssystem-Abbilder werden in einem freigegebenen Ordner auf dem Administrationsserver gespeichert. Das Aufzeichnen und das Erstellen eines Betriebssystem-Abbilds eines Mustergeräts erfolgt mit der Aufgabe zum Erstellen eines Installationspakets (s. Abschnitt "Installationspakete für Programme erstellen" auf S. 264).

> Um Betriebssystem-Abbilder erstellen zu können, muss das Windows Automated Installation Kit (WAIK) auf dem Administrationsserver installiert werden.

Die Funktion zum Aufzeichnen eines Betriebssystem-Abbilds weist folgende Besonderheiten auf:

- Es kann kein Betriebssystem-Abbild des Geräts erstellt werden, auf dem der Administrationsserver installiert wurde.
- Beim Erstellen eines Betriebssystem-Abbilds werden die Einstellungen des Mustergeräts durch das Tool sysprep.exe zurückgesetzt. Wenn die Einstellungen eines Mustergeräts wiederhergestellt werden sollen, müssen Sie im Assistenten für das Erstellen von Betriebssystem-Images das Kontrollkästchen **Backup-Kopie des Gerätestatus speichern** aktivieren.
- Beim Erstellen des Abbilds wird ein Neustart des Mustergeräts durchgeführt.

Betriebssystem-Abbilder auf neuen Geräten verteilen

Der Administrator kann die erstellten Abbilder auf neue Geräte des Netzwerks verteilen, auf denen noch kein Betriebssystem installiert wurde. Dazu wird die Technologie Preboot eXecution Environment (PXE) verwendet. Der Administrator bestimmt ein Gerät im Netzwerk, das als PXE-Server verwendet werden soll. Dieses Gerät muss folgende Voraussetzungen erfüllen:

- Auf dem Gerät muss der Administrationsagent installiert sein.
- Auf dem Gerät darf kein DHCP-Server laufen, da der PXE-Server dieselben Ports verwendet wie der DHCP-Server.
- Im Netzwerksegment, zu dem das Gerät gehört, dürfen keine anderen PXE-Server vorhanden sein.

Um ein Betriebssystem zu verteilen, ist es erforderlich, eine Netzwerkkarte auf dem Gerät zu installieren, das Gerät ans Netzwerk anzuschließen und beim Hochfahren des Geräts in der BIOS-Umgebung die Installationsvariante Netzwerkstart auszuwählen.

Die Verteilung des Betriebssystems erfolgt in folgender Reihenfolge:

1. Der PXE-Server stellt eine Verbindung mit einem neuen Client-Gerät bei seinem Neustart her.
2. Das Client-Gerät wird in die Windows-Vorinstallationsumgebung (WinPE) aufgenommen.

   > Um ein Gerät in die WinPE-Umgebung einzubinden, müssen Sie ggf. die Treiber für die WinPE-Umgebung anpassen.

3. Das Client-Gerät wird auf dem Administrationsserver registriert.

4. Der Administrator weist dem Client-Gerät ein Installationspaket mit dem Abbild des Betriebssystems zu.

   > Der Administrator kann die erforderlichen Treiber zum Installationspaket mit dem Betriebssystem-Abbild hinzufügen und die Konfigurationsdatei mit den Einstellungen für das Betriebssystem vorgeben, die für die Installation angewendet werden sollen.

5. Das Betriebssystem wird auf dem Client-Gerät verteilt.

Der Administrator kann MAC-Adressen der noch nicht verbundenen Client-Geräte manuell angeben und das Installationspaket mit dem Abbild des Betriebssystems den Geräten zuweisen. Bei der Verbindung der Client-Geräte mit dem PXE-Server wird das Betriebssystem automatisch auf diesen Geräten installiert.

Betriebssystem-Images auf Geräten mit einem bereits installierten Betriebssystem verteilen

Die Verteilung der Betriebssystem-Abbilder auf Client-Geräten mit einem bereits installierten Betriebssystem erfolgt mit einer Aufgabe zur Remote-Installation für bestimmte Geräte.

Kaspersky-Lab-Programme und Programme anderer Software-Hersteller installieren

Der Administrator kann für beliebige Programme, unter anderem für vom Benutzer angegebene Programme, Installationspakete erstellen und diese Programme mit einer Aufgabe zur Remote-Installation auf den Client-Geräten installieren.

In diesem Abschnitt

Betriebssystem-Abbilder erstellen

Das Erstellen von Betriebssystem-Abbildern erfolgt mit der Aufgabe zum Erfassen eines Betriebssystem-Abbilds des Mustergeräts.

Gehen Sie wie folgt vor, um eine Aufgabe zum Erfassen eines Betriebssystem-Abbilds anzulegen:

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

2. Starten Sie über den Link **Installationspaket erstellen** den Assistenten für das Erstellen von Installationspaketen.

3. Klicken Sie im Fenster des Assistenten **Typ des Installationspakets auswählen** auf die Schaltfläche **Installationspaket auf Basis eines Betriebssystem-Images erstellen**.

4. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe des Administrationsservers **Betriebssystem-Abbild eines Mustergeräts erzeugen** erstellt. Sie können sich die Aufgabe im Ordner **Aufgaben** anzeigen lassen.

Nach Fertigstellung der Aufgabe **Betriebssystem-Abbild eines Mustergeräts erzeugen** wird das Installationspaket erstellt, das Sie zur Verteilung des Betriebssystems auf den Client-Geräten mithilfe eines PXE-Servers oder einer Aufgabe zur Remote-Installation verwenden können.
Sie können das Installationspaket im Ordner **Installationspakete** ansehen.

Treiber für die Windows-Vorinstallationsumgebung (WinPE) hinzufügen

Um Treiber für die WinPE-Umgebung hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** den Unterordner **Images von Geräten verteilen** aus.

2. Klicken Sie im Arbeitsplatz des Ordners **Images von Geräten verteilen** klicken Sie auf die Schaltfläche **Erweiterte Aktionen** und wählen Sie in der Dropdown-Liste den Punkt **Synchronisierung von Windows-Updates anpassen** aus.

   Daraufhin wird das Fenster **Treiber für die Windows-Vorinstallationsumgebung** geöffnet.

3. Klicken Sie im Fenster **Treiber für die Windows-Vorinstallationsumgebung** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Treiber hinzufügen** wird geöffnet.

4. Geben Sie im Fenster **Treiber hinzufügen** den Namen und den Pfad für das Installationspaket des Treibers ein. Die Eingabe des Pfads für das Installationspaket des Treibers erfolgt über die Schaltfläche **Auswählen** im Fenster **Treiber hinzufügen**.

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

   Der Treiber wird zur Datenverwaltung des Administrationsservers hinzugefügt. Der neu hinzugefügte Treiber wird im Fenster **Treiber auswählen** angezeigt.

6. Klicken Sie im Fenster **Treiber auswählen** auf die Schaltfläche **OK**.

Der Treiber wird zur Windows-Vorinstallationsumgebung (WinPE) hinzugefügt.

Treiber zum Installationspaket mit dem Betriebssystem-Abbild hinzufügen

Um Treiber zum Installationspaket mit dem Betriebssystem-Abbild hinzuzufügen, gehen Sie folgendermaßen vor.

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

2. Klicken Sie mit der rechten Maustaste auf das Installationspaket mit dem Betriebssystem-Abbild und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Installationspakets wird geöffnet.

3. Wählen Sie im Eigenschaftsfenster des Installationspakets den Bereich **Zusätzliche Treiber**.

4. Klicken Sie im Abschnitt **Zusätzliche Treiber** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Treiber auswählen** wird geöffnet.

5. Wählen Sie im Fenster **Treiber auswählen** die Treiber aus, die Sie zum Installationspaket des Betriebssystem-Abbildes hinzufügen möchten.

   Sie können neue Treiber zur Datenverwaltung des Administrationsservers hinzufügen, indem Sie auf die Schaltfläche **Hinzufügen** im Fenster **Treiber auswählen** klicken.

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

Die neu hinzugefügten Treiber werden unter **Zusätzliche Treiber** im Eigenschaftsfenster des Installationspakets mit dem Betriebssystem-Abbild angezeigt.

Einstellungen des Tools sysprep.exe anpassen

Das Tool sysrep.exe wird für die Vorbereitung des Geräts auf das Erstellen seines Betriebssystemabbildes verwendet.

Um die Einstellungen für das Tool sysprep.exe anzupassen, gehen Sie wie folgt vor:

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

2. Klicken Sie mit der rechten Maustaste auf das Installationspaket mit dem Betriebssystem-Abbild und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Installationspakets wird geöffnet.

3. Wählen Sie im Eigenschaftsfenster des Installationspakets den Bereich **Einstellungen für sysprep.exe**.

4. Geben Sie im Abschnitt **Einstellungen für sysprep.exe** die Konfigurationsdatei an, die für die Installation des Betriebssystems auf dem Client-Gerät verwendet werden soll:

   - **Standard-Konfigurationsdatei verwenden**. Wählen Sie diese Option, wenn Sie die Antwortdatei verwenden möchten, die standardmäßig bei der Aufzeichnung des Betriebssystem-Abbilds erstellt wird.

   - **Benutzerdefinierte Werte der wichtigsten Einstellungen festlegen**. Wählen Sie diese Option, um die Einstellungswerte anhand der Benutzeroberfläche festzulegen.

   - **Konfigurationsdatei angeben**. Wählen Sie diese Option, um eine eigene Konfigurationsdatei zu verwenden.

5. Klicken Sie auf die Schaltfläche **Übernehmen**, damit die vorgenommenen Änderungen wirksam werden.

Betriebssysteme auf neue Geräte des Netzwerks verteilen

Gehen Sie wie folgt vor, um ein Betriebssystem auf neue Geräte zu verteilen, auf denen noch kein Betriebssystem installiert wurde:

1. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** den Unterordner **Images von Geräten verteilen** aus.

2. Klicken Sie auf die Schaltfläche **Erweiterte Aktionen** und wählen Sie in der Dropdown-Liste den Punkt **Liste der PXE-Server im Netzwerk verwalten** aus.

   Dieser Link öffnet das Fenster **Eigenschaften**: **Images von Geräten verteilen** mit dem Abschnitt **PXE-Server**.

3. Klicken Sie im Abschnitt **PXE-Server** auf die Schaltfläche **Hinzufügen** und wählen Sie im folgenden Fenster **PXE-Server** das Gerät aus, das als PXE-Server verwendet werden soll.

   Das hinzugefügte Gerät wird im Abschnitt PXE-Server angezeigt.

4. Wählen Sie im Abschnitt **PXE-Server** den PXE-Server aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.

5. Passen Sie im Eigenschaftenfenster des gewählten PXE-Servers im Abschnitt **Einstellungen für die Verbindung zum PXE-Server** die Einstellungen für die Verbindung des Administrationsservers mit dem PXE-Server an.

6. Starten Sie das Client-Gerät, auf dem Sie das Betriebssystem installieren möchten.

7. Wählen Sie in der BIOS-Umgebung des Client-Geräts die Installationsvariante Netzwerkstart aus.

   Das Client-Gerät wird mit dem PXE-Server verbunden und im Arbeitsplatz des Ordners **Images von Geräten verteilen** angezeigt.

8. Wählen Sie im Abschnitt **Aktionen** durch Klicken auf den Link **Installationspaket bestimmen** das Installationspaket aus, das für die Installation des Betriebssystems auf dem gewählten Gerät verwendet werden soll.

   Sobald das Gerät hinzugefügt und ein Installationspaket dafür bestimmt wurde, beginnt die Installation des Betriebssystems auf diesem Gerät automatisch.

9. Um die Installation des Betriebssystems auf dem Client-Gerät abzubrechen, klicken Sie im Abschnitt **Aktionen** auf den Link **Installation von Betriebssystem-Abbildern abbrechen**.

Um ein Gerät nach seiner MAC-Adresse hinzuzufügen,

- klicken Sie im Ordner **Images von Geräten verteilen** auf den Link **MAC-Adresse des Zielgeräts hinzufügen** und geben Sie im folgenden Fenster **Neues Gerät** die MAC-Adresse des Geräts an, das Sie hinzufügen möchten

- wählen Sie durch Klicken auf den Link **Mac-Adressen der Geräte aus Datei importieren** im Ordner **Images von Geräten verteilen** die Datei aus, welche die Liste der MAC-Adressen aller Geräte enthält, auf denen Sie das Betriebssystem installieren möchten.

Betriebssysteme auf Client-Geräte verteilen

Gehen Sie wie folgt vor, um ein Betriebssystem auf Client-Geräte zu verteilen, auf denen ein Betriebssystem bereits installiert ist:

1. Starten Sie in der Konsolenstruktur im Ordner **Remote-Installation** über den Link **Installationspakete auf den verwalteten Geräten (Arbeitsplätzen) verteilen** den Assistenten zur Softwareverteilung.

2. Geben Sie im Fenster des Assistenten **Installationspaket auswählen** das Installationspaket mit dem Betriebssystem-Abbild an.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe zur Remote-Installation des Betriebssystems auf Client-Geräten erstellt. Sie können die Aufgabe im Ordner **Aufgaben** starten oder beenden.

Installationspakete für Programme erstellen

Gehen Sie wie folgt vor, um ein Installationspaket für ein Programm zu erstellen:

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

2. Starten Sie über den Link **Installationspaket erstellen** den Assistenten für das Erstellen von Installationspaketen.

3. Klicken Sie im Fenster des Assistenten **Typ des Installationspakets auswählen** auf eine der folgenden Schaltflächen:

   - **Installationspaket für Kaspersky-Lab-Anwendung erstellen**. Wählen Sie diese Option aus, wenn Sie das Installationspaket für ein Kaspersky-Lab-Programm erstellen möchten.

   - **Installationspaket für die benutzerdefinierte Anwendung erstellen**. Wählen Sie diese Option aus, wenn Sie das Installationspaket für ein vom Benutzer angefordertes Programm erstellen möchten.

   - **Installationspaket mit dem Betriebssystem-Abbild eines Mustergeräts erstellen**. Wählen Sie diese Option aus, wenn Sie das Installationspaket mit dem Betriebssystem-Abbild eines Mustergeräts erstellen möchten.

     Nach Abschluss des Assistenten wird die Aufgabe des Administrationsservers **Betriebssystem-Abbild eines Mustergeräts erzeugen** erstellt. Nach Fertigstellung der Aufgabe wird ein Installationspaket erstellt, das zur Verteilung des Betriebssystem-Abbilds mithilfe eines PXE-Servers oder einer Aufgabe zur Remote-Installation verwendet werden kann.

4. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird ein Installationspaket erstellt, das für die Installation des Programms auf den Client-Geräten verwendet werden kann. Sie können das Installationspaket im Ordner **Installationspakete** ansehen.

Nähere Informationen zu Installationspaketen finden Sie im *Implementierungshandbuch von Kaspersky Security Center*.

Ausgabe eines Zertifikats für Installationspakete von Programmen

Gehen Sie wie folgt vor, um ein Zertifikat für ein Installationspaket eines Programms auszustellen:

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 mit der rechten Maustaste auf den Ordner **Installationspakete** und wählen Sie den Punkt **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster des Ordners **Installationspakete** geöffnet.

3. Wählen Sie im Eigenschaftenfenster des Ordners **Installationspakete** den Abschnitt **Signatur der autonomen Pakete** aus.

4. Klicken Sie im Abschnitt **Signatur der autonomen Pakete** auf die Schaltfläche **Festlegen**.

   Daraufhin öffnet sich das Fenster **Zertifikat**.

5. Wählen Sie im Feld **Zertifikatstyp** entweder einen offenen oder geschlossenen Zertifikatstyp aus.

   - Wenn der Wert **Container PKCS#12** ausgewählt ist, geben Sie die Zertifikatsdatei und das Kennwort an.

   - Wenn der Wert **X.509-Zertifikat** ausgewählt ist:

     a. Geben Sie die Datei des privaten Schlüssels an (Datei mit der Erweiterung prk oder pem).

     b. Geben Sie das Kennwort des privaten Schlüssels an.

     c. Geben Sie die Datei des offenen Schlüssel an (Datei mit der Erweiterung cer).

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

Daraufhin wird ein Zertifikat für das Installationspaket des Programms ausgestellt.

Programme auf Client-Geräten installieren

Gehen Sie wie folgt vor, um ein Programm auf Client-Geräten zu installieren:

1. Starten Sie in der Konsolenstruktur im Ordner **Remote-Installation** über den Link **Installationspakete auf den verwalteten Geräten (Arbeitsplätzen) verteilen** den Assistenten zur Softwareverteilung.

2. Geben Sie im Fenster des Assistenten **Installationspaket auswählen** das Installationspaket für das Programm an, das Sie installieren möchten.

3. Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wird die Aufgabe zur Remote-Installation des Programms auf den Client-Geräten angelegt. Sie können die Aufgabe im Ordner **Aufgaben** starten oder beenden.

Sie können den Administrationsagenten auf Client-Geräten mit den Betriebssystemen Windows, Linux und MacOS mithilfe des Softwareverteilungs-Assistenten installieren.

Vor dem Ausführen der Remote-Installation des Administrationsagenten auf einem Gerät mit dem Betriebssystem Linux muss das Gerät vorbereitet werden (s. Abschnitt "Ein Gerät mit dem Betriebssystem Linux für die Remote-Installation des Administrationsagenten vorbereiten" s. S. 397).

Mobile Geräte verwalten

In diesem Abschnitt wird beschrieben, wie Sie mobile Geräte verwalten können, die mit dem Administrationsserver verbunden sind. Informationen zur Verbindung von mobilen Geräten können Sie dem *Kaspersky Security Center Implementierungshandbuch* entnehmen.

In diesem Abschnitt

Mobile Geräte mithilfe der MDM-Richtlinie verwalten

Sie können zur Verwaltung von iOS MDM- und EAS-Geräten das Verwaltungs-Plug-in von Kaspersky Mobile Device Management 10 Service Pack 1 verwenden, das zum Lieferumfang von Kaspersky Security Center gehört. Mithilfe von Kaspersky Mobile Device Management können Sie Gruppenrichtlinien zum Anpassen von Konfigurationseinstellungen für iOS MDM- und EAS-Geräte erstellen. Eine Gruppenrichtlinie, mit der die Konfigurationseinstellungen für iOS MDM- und EAS-Geräte ohne Verwendung der iPhone Configuration Utility bzw. des Exchange Active Sync-Verwaltungsprofils angepasst werden können, wird als MDM-Richtlinie bezeichnet.

Eine MDM-Richtlinie gibt dem Administrator folgende Möglichkeiten:

- für die Verwaltung von EAS-Geräten:
  - Kennworteinstellungen für die Entsperrung des Geräts anpassen
  - Speicherung von Daten in verschlüsselter Form auf dem Gerät anpassen
  - Einstellungen für die Synchronisierung der Unternehmens-E-Mail anpassen
  - Hardwarefunktionen der mobilen Geräte anpassen, beispielsweise Nutzung von Wechseldatenträgern, Verwendung der Kamera, Verwendung von Bluetooth
  - Beschränkungen für die Nutzung von mobilen Apps auf dem Gerät anpassen.
- für die Verwaltung von iOS MDM-Geräten:
  - Sicherheitseinstellungen für die Verwendung des Kennworts auf dem Gerät anpassen
  - Beschränkungen für die Verwendung der Hardwarefunktionen des Geräts sowie Beschränkungen für die Installation und Deinstallation von mobilen Apps anpassen
  - Beschränkungen für die Verwendung der auf dem Gerät integrierten mobilen Apps, beispielsweise YouTube™, iTunes Store, Safari, anpassen
  - Beschränkungen für die Anzeige von Medieninhalten (beispielsweise Filme und Fernsehsendungen) nach der Region anpassen, in der das Gerät benutzt wird
  - Internetverbindungseinstellungen des Geräts über einen Proxyserver (Globaler HTTP-Proxy) anpassen
  - Einstellungen für ein Einmalbenutzerkonto anpassen, mit dem der Benutzer Zugang zu Apps und Diensten des Unternehmens erhält (Technologie zur Einmalanmeldung)
  - Internetnutzung (Besuch von Websites) auf den mobilen Geräten kontrollieren
  - Einstellungen von kabellosen Netzwerken (WLAN), Zugriffspunkten (APN), virtuellen privaten Netzwerken (VPN) mithilfe verschiedenster Authentifizierungsmechanismen und Netzwerkprotokollen anpassen

- Verbindungseinstellungen von AirPlay-Geräten zum Streamen von Fotos, Musik und Videos anpassen
- Verbindungseinstellungen von AirPrint-Druckern zum kabellosen Drucken von Dokumenten vom Gerät anpassen
- Synchronisierungseinstellungen mit dem Microsoft Exchange-Server sowie Benutzerkonten für die Nutzung der Unternehmens-E-Mail auf den Geräten anpassen
- Anmeldedaten für die Synchronisierung mit dem Katalogdienst LDAP anpassen
- Anmeldedaten für die Verbindung mit den Diensten CalDAV und CardDAV anpassen, wodurch der Benutzer Unternehmenskalender und Kontaktlisten verwenden kann
- Einstellungen der iOS-Benutzeroberfläche auf dem Benutzergerät anpassen, beispielsweise Schriftarten oder Symbole für ausgewählte Websites
- Neue Sicherheitszertifikate zum Gerät hinzufügen
- Einstellungen des SCEP-Servers für den automatischen Erhalt von Zertifikaten von der Zertifizierungsstelle anpassen
- Eigene Einstellungen für die Ausführung von mobilen Apps hinzufügen.

Die allgemeinen Prinzipien für MDM-Richtlinien unterscheiden sich nicht von den Prinzipien für Richtlinien, die für die Verwaltung anderer Programme erstellt wurden. Die Besonderheit der MDM-Richtlinie liegt darin, dass sie einer Administrationsgruppe zugewiesen wird, zu der der iOS MDM-Server und der Exchange ActiveSync-Server für mobile Geräte gehören (im Folgenden Server für mobile Geräte). Alle Einstellungen, die in der MDM-Richtlinie festgelegt sind, werden zunächst auf die Server für mobile Geräte und dann auf die von ihnen verwalteten mobilen Geräte angewendet. Falls eine hierarchische Struktur von Administrationsgruppen verwendet wird, erhalten die untergeordneten Server für mobile Geräte die Einstellungen der MDM-Richtlinie von den Hauptservern für mobile Geräte und verteilen sie auf die mobilen Geräte.

Nähere Informationen über die MDM-Richtlinie in der Verwaltungskonsole von Kaspersky Security Center finden Sie im Administratorhandbuch zur Komplexlösung Kaspersky Security für mobile Endgeräte.

Arbeiten mit Befehlen für mobile Geräte

Dieser Abschnitt enthält Informationen über die Befehle für die Verwaltung von mobilen Geräten, die vom Programm unterstützt werden. Es werden Anleitungen für das Versenden der Befehle an die mobilen Geräte sowie für die Anzeige des Ausführungsstatus der Befehle im Befehlsprotokoll angeführt.

Befehle zur Verwaltung von mobilen Geräten

Im Programm werden Befehle zur Verwaltung von mobilen Geräten unterstützt.

Die Befehle werden für die ferngesteuerte Verwaltung von mobilen Geräten verwendet. Im Fall des Verlusts eines mobilen Geräts können mithilfe von Befehlen beispielsweise Unternehmensdaten vom Gerät gelöscht werden.

Die Befehle werden auf drei Typen von mobilen Geräten verwendet:

- iOS MDM-Gerät
- KES-Gerät
- EAS-Gerät.

Jeder Gerätetyp unterstützt eine bestimmte Auswahl von Befehlen. In der Tabelle unten ist die Liste der Befehle für jeden Typ der mobilen Geräte angeführt.

Für alle Gerätetypen werden bei erfolgreicher Ausführung des Befehls **Auf Werkseinstellungen zurücksetzen** alle Daten vom mobilen Gerät gelöscht und die Geräteeinstellungen auf Werkseinstellungen zurückgesetzt.

Für das iOS MDM-Gerät werden bei erfolgreicher Ausführung des Befehls **Unternehmensdaten löschen** alle voreingestellten Konfigurationsprofile, Provisioning-Profile, das iOS MDM-Profil und die Apps, für die das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert wurde, gelöscht.

Für das KES-Gerät werden bei erfolgreicher Ausführung des Befehls **Unternehmensdaten löschen** die Unternehmensdaten, Einträge in Kontakten, der SMS-Verlauf, die Anrufliste, der Kalender, die Einstellungen für die Internetverbindung, die Benutzerkonten mit Ausnahme des Google-Benutzerkontos vom mobilen Gerät gelöscht. Außerdem werden für das KES-Gerät die Daten von der Speicherkarte gelöscht.

Tabelle 2. Liste der unterstützten Befehle

Typ des mobilen Geräts	Befehle	Ergebnis der Befehlsausführung
iOS MDM-Gerät	Blockieren	Das mobile Gerät wurde gesperrt.
	Entsperren	Blockierung des mobilen Geräts mit PIN-Code ist deaktiviert. Der früher festgelegte PIN-Code wurde zurückgesetzt.
	Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des Geräts wurden auf die Werkseinstellung zurückgesetzt
	Unternehmensdaten löschen	Alle installierten Konfigurationsprofile, Provisioning-Profile, iOS MDM-Profile und Apps, für die das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert ist, wurden gelöscht.
	Gerät synchronisieren	Die Daten auf dem mobilen Gerät wurden mit dem Administrationsserver synchronisiert.
	Profil installieren	Auf dem mobilen Gerät wurde ein Konfigurationsprofil installiert.
	Profil entfernen	Das Konfigurationsprofil wurde vom mobilen Gerät gelöscht.
	Provisioning-Profil installieren	Auf dem mobilen Gerät wurde ein Provisioning-Profil installiert.

Typ des mobilen Geräts	Befehle	Ergebnis der Befehlsausführung
	Provisioning-Profil löschen	Das Provisioning-Profil wurde vom mobilen Gerät gelöscht.
	App installieren	Auf dem mobilen Gerät wurde eine App installiert.
	App löschen	Die App wurde vom mobilen Gerät gelöscht.
	Gutscheincode eingeben	Ein Gutscheincode für eine kostenpflichtige App wurde eingegeben.
	Roaming konfigurieren	Daten-Roaming und Sprach-Roaming wurden aktiviert bzw. deaktiviert.
	Kaspersky Safe Browser installieren	Die App Kaspersky Safe Browser ist auf dem mobilen Gerät installiert.
KES-Gerät	Blockieren	Das mobile Gerät wurde gesperrt.
	Entsperren	Blockierung des mobilen Geräts mit PIN-Code ist deaktiviert. Der früher festgelegte PIN-Code wurde zurückgesetzt.
	Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf die Werkseinstellung zurückgesetzt.
	Unternehmensdaten löschen	Alle installierten Konfigurationsprofile, Provisioning-Profile, iOS MDM-Profile und Apps, für die das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert ist, wurden gelöscht.
	Gerät synchronisieren	Die Daten auf dem mobilen Gerät wurden mit dem Administrationsserver synchronisiert.

Typ des mobilen Geräts	Befehle	Ergebnis der Befehlsausführung
	Standort ermitteln	Der Standort des mobilen Geräts wurde ermittelt und auf Google Maps™ angezeigt. Der Mobilfunkanbieter erhebt Gebühren für den SMS-Versand und die Verbindung mit dem Internet.
	Bild aufnehmen	Das mobile Gerät wurde gesperrt. Mit der Frontkamera des Geräts wurde ein Foto aufgenommen und auf dem Administrationsserver gespeichert. Die Fotos können im Befehlsprotokoll angezeigt werden. Der Mobilfunkanbieter erhebt Gebühren für den SMS-Versand und die Verbindung mit dem Internet.
	Tonsignal wiedergeben	Das mobile Gerät gibt ein Tonsignal wieder.
EAS-Gerät	Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen des mobilen Geräts wurden auf die Werkseinstellung zurückgesetzt.

Verwendung von Google Firebase Cloud Messaging

Zur rechtzeitigen Zustellung von Befehlen auf KES-Geräten unter dem Betriebssystem Android wird in Kaspersky Security Center das System der Push-Benachrichtigung verwendet. Push-Benachrichtigungen zwischen KES-Geräten und dem Administrationsserver werden mithilfe des Dienstes Google Firebase Cloud Messaging realisiert.

In der Kaspersky Security Center Verwaltungskonsole können Sie die Einstellungen für den Dienst Google Firebase Cloud Messaging festlegen, um KES-Geräte an diesen Dienst zu anzuschließen.

Um die Einstellungen für Google Firebase Cloud Messaging zu erhalten, muss der Administrator über ein Google-Benutzerkonto verfügen. Detailliertere Informationen über den Erhalt der Einstellungen für Google Firebase Cloud Messaging finden Sie im entsprechenden Artikel der Wissensdatenbank auf der Website des Technischen Supports unter http://support.kaspersky.com/de/11770.

Um die Einstellungen für Google Firebase Cloud Messaging anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

2. Klicken Sie mit der rechten Maustaste auf den Ordner **Mobile Geräte** und wählen Sie den Punkt **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster des Ordners **Mobile Geräte** geöffnet.

3. Wählen Sie den Abschnitt **Einstellungen für Google Firebase Cloud Messaging** aus.

4. Geben Sie im Feld **Absender-ID** die Google-API-Projektnummer ein, die Sie bei der Erstellung des Projekts in der Google-Entwicklerkonsole erhalten haben.

5. Geben Sie im Feld **API-Schlüssel** den gewöhnlichen API-Schlüssel an, den Sie in der Google-Entwicklerkonsole erstellt haben.

Bei der nächsten Synchronisierung mit dem Administrationsserver werden KES-Geräte unter dem Betriebssystem Android an den Dienst Google Firebase Cloud Messaging angeschlossen.

Sie können die Einstellungen für Google Firebase Cloud Messaging mithilfe der Schaltfläche **Einstellungen zurücksetzen** ändern.

Befehle absenden

Gehen Sie wie folgt vor, um einen Befehl an ein mobiles Gerät des Benutzers zu senden:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Wählen Sie das mobile Gerät des Benutzers, an das der Befehl gesendet werden soll.

3. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

4. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt mit dem Namen des Befehls, der an das mobile Gerät gesendet werden soll, und klicken Sie auf die Schaltfläche **Befehl senden**.

   Nachdem Sie auf die Schaltfläche **Befehl senden** geklickt haben, öffnet sich abhängig vom ausgewählten Befehl möglicherweise das Fenster zum Anpassen der erweiterten Einstellungen des Befehls. Wenn zum Beispiel der Befehl zum Löschen des Provisioning-Profils gesendet wird, müssen Sie das Provisioning-Profil auswählen, das vom mobilen Gerät gelöscht werden soll. Geben Sie im Fenster die erweiterten Einstellungen des Befehls ein und bestätigen Sie Ihre Auswahl. Daraufhin wird der Befehl an das mobile Gerät gesendet.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

5. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle für die Verwaltung des Mobilgeräts** zu schließen.

Status von Befehlen im Befehlsprotokoll anzeigen

Im Befehlsprotokoll werden Informationen über alle Befehle gespeichert, die an mobile Geräte gesendet wurden. Das Befehlsprotokoll enthält Informationen über Uhrzeit und Datum der Absendung des Befehls an das mobile Gerät, Status der Befehle sowie eine detaillierte Beschreibung der Ergebnisse der Befehlsausführung. Beispielsweise wird im Fall der fehlerhaften Ausführung des Befehls im Befehlsprotokoll die Fehlerursache angezeigt. Die Einträge im Befehlsprotokoll werden nach 30 Tagen gelöscht.

Die an ein mobiles Gerät gesendeten Befehle können folgende Status aufweisen:

- *Wird ausgeführt* – der Befehl wurde an das mobile Gerät gesendet.
- *Abgeschlossen* – der Befehl wurde erfolgreich ausgeführt.
- *Beendet mit Fehler* – der Befehl konnte nicht ausgeführt werden.
- *Wird gelöscht* – der Befehl wird aus der an das mobile Gerät gesendeten Befehlswarteschlange gelöscht.
- *Gelöscht* – der Befehl wurde erfolgreich aus der an das mobile Gerät gesendeten Befehlswarteschlange gelöscht.
- *Löschen fehlgeschlagen* – der Befehl konnte nicht aus der an das mobile Gerät gesendeten Befehlswarteschlange gelöscht werden.

Das Programm führt für jedes mobile Gerät ein Befehlsprotokoll.

Gehen Sie wie folgt vor, um das Befehlsprotokoll für an ein mobiles Gerät gesendete Befehle anzuzeigen:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Wählen Sie das mobile Gerät, für das Sie das Befehlsprotokoll anzeigen möchten, aus der Liste.

3. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

   Das Fenster **Befehle zur Verwaltung von mobilen Geräten** wird geöffnet. Die Abschnitte im Fenster **Befehle zur Verwaltung von mobilen Geräten** entsprechen den Befehlen, die an ein mobiles Gerät gesendet werden können.

4. Wählen Sie die Abschnitte mit den gewünschten Befehlen und lesen Sie im Block **Befehlsprotokoll** die Informationen über deren Ausführung.

Im Block **Befehlsprotokoll** werden eine Liste der an das mobile Gerät gesendeten Befehle sowie Informationen zu den Befehlen angezeigt. Mithilfe des Filters **Befehle zeigen** können Sie in der Liste nur Befehle mit dem ausgewählten Status anzeigen.

Arbeiten mit Zertifikaten

Dieser Abschnitt enthält Informationen über die Arbeit mit Zertifikaten für mobile Geräte. Hier finden Sie Anweisungen zur Installation von Zertifikaten auf den mobilen Geräten des Benutzers und zur Anpassung der Regeln für die Ausstellung von Zertifikaten. Ferner enthält dieser Abschnitt Anweisungen zur Integration des Programms mit einer Public-Key-Infrastruktur sowie zur Konfiguration der Kerberos-Unterstützung.

Zertifikat installieren

Auf den mobilen Geräten des Benutzers können drei Typen von Zertifikaten installiert werden:

- allgemeine Zertifikate zur Identifizierung des mobilen Geräts
- E-Mail-Zertifikate für die Konfiguration der Unternehmens-E-Mail auf dem mobilen Gerät
- VPN-Zertifikate für die Konfiguration des Zugriffs auf ein virtuelles privates Netzwerk auf dem mobilen Gerät.

Gehen Sie wie folgt vor, um ein Zertifikat auf einem mobilen Gerät des Benutzers zu installieren:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten** und wählen Sie den Unterordner **Zertifikate** aus.

2. Starten Sie im Arbeitsplatz des Ordners **Zertifikate** mithilfe des Links **Zertifikat hinzufügen** den Assistenten zur Zertifikatinstallation.

Folgen Sie den Anweisungen des Assistenten.

Nach Abschluss des Assistenten wurde ein Zertifikat erstellt, zur Liste der Zertifikate des Benutzers hinzugefügt, und außerdem eine Benachrichtigung mit einem Link für den Download und die Installation des Zertifikats auf dem mobilen Gerät an den Benutzer gesendet. Eine Liste aller Zertifikate kann angezeigt und in eine Datei exportiert werden (s. Abschnitt "Liste der für den Benutzer ausgestellten Zertifikate anzeigen" auf S. 191). Zertifikate können gelöscht und erneut ausgestellt werden. Darüber hinaus können Sie auch die Eigenschaften eines Zertifikats anzeigen.

Regeln für die Ausstellung eines Zertifikats anpassen

Um die Regeln für die Ausstellung eines Zertifikats anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten** und wählen Sie den Unterordner **Zertifikate** aus.

   Der Ordner **Mobile Geräte verwalten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Öffnen Sie im Arbeitsplatz des Ordners **Zertifikate** mithilfe der Schaltfläche **Regeln für die Ausstellung eines Zertifikats anpassen-**das Fenster **Regeln für das Ausstellen von Zertifikaten**.

3. Gehen Sie zum Abschnitt mit dem Namen des Zertifikatstyps:

   Allgemeine Zertifikate ausstellen – für die Anpassung der Ausstellung allgemeiner Zertifikate

   E-Mail-Zertifikate ausstellen – für die Anpassung der Ausstellung von E-Mail-Zertifikaten

   Ausstellung von VPN-Zertifikaten – für die Anpassung der Ausstellung von VPN-Zertifikaten.

4. Passen Sie im Block **Ausstellungseinstellungen** die Ausstellung der Zertifikate wie folgt an:

   - Geben Sie die Gültigkeitsdauer des Zertifikats in Tagen an.
   - Wählen Sie die Quelle für die Zertifikate aus (**Administrationsserver** oder **Zertifikate werden manuell erstellt**).

     Standardmäßig ist der Administrationsserver als Quelle für die Zertifikate ausgewählt.

   - Geben Sie eine Zertifikatsvorlage an (**Standardvorlage**, **Andere Vorlage**).

     Die Anpassung von Vorlagen ist verfügbar, wenn im Abschnitt **PKI-Integration** die Integration mit Public Key-Infrastruktur ausgewählt ist (auf S. 280).

5. Passen Sie im Block **Einstellungen für das automatische Update** das automatische Update des Zertifikats an:

   - Geben Sie im Block **Frist zur Erneuerung vor Ablauf der Gültigkeitsdauer (Tage)** an, wie viele Tage vor Ablauf der Gültigkeitsdauer das Zertifikat aktualisiert werden muss.
   - Um das automatische Update von Zertifikaten zu aktivieren, aktivieren Sie das Kontrollkästchen **Zertifikat automatisch neu veröffentlichen, falls möglich**.

   Ein allgemeines Zertifikat kann nur manuell neu ausgestellt werden.

6. Aktivieren und konfigurieren Sie im Block **Verschlüsselungseinstellungen** die Verschlüsselung der ausgestellten Zertifikate.

   > Die Verschlüsselung ist nur für allgemeine Zertifikate verfügbar.

   a. Aktivieren Sie das Kontrollkästchen **Verschlüsselung für Zertifikate aktivieren**.

   b. Passen Sie mithilfe des Schiebereglers die maximale Anzahl von Zeichen im Kennwort für die Verschlüsselung an.

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

Integration mit Public-Key-Infrastruktur

Die Integration mit Public-Key-Infrastruktur (PKI) ist erforderlich, um die Ausstellung von Domänenzertifikaten der Benutzer zu vereinfachen. Die Integration der Zertifikatausstellung erfolgt daraufhin automatisch.

Das Benutzerkonto muss für die Integration mit PKI angepasst werden. Das Benutzerkonto muss folgenden Anforderungen genügen:

- Es muss Domänenbenutzer und Administrator des Geräts sein, auf dem der Administrationsserver installiert ist.
- Es muss auf dem Gerät mit dem installierten Administrationsserver über die Berechtigung SeServiceLogonRight verfügen.

Mit dem vorkonfigurierten Benutzerkonto muss auf dem Gerät, auf dem der Administrationsserver installiert ist, mindestens einmal eine Anmeldung durchgeführt werden, um ein ständiges Benutzerprofil zu erstellen. Im Zertifikatsspeicher dieses Benutzers auf dem Gerät mit dem Administrationsserver muss ein Zertifikat des Registrierungsagenten installiert werden, das von den Domänenadministratoren zur Verfügung gestellt wird.

Um die Integration mit Public-Key-Infrastruktur anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten** und wählen Sie den Unterordner **Zertifikate** aus.

   Der Ordner **Mobile Geräte verwalten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Öffnen Sie im Arbeitsplatz mithilfe der Schaltfläche **In Public-Key-Infrastruktur integrieren** den Abschnitt **PKI-Integration** im Fenster **Regeln für das Ausstellen von Zertifikaten**.

   Daraufhin wird der Abschnitt **PKI-Integration** des Fensters **Regeln für das Ausstellen von Zertifikaten** geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Zertifikatsausstellung in die PKI integrieren**.

4. Geben Sie im Feld **Benutzerkonto** den Kontonamen des Benutzerkontos an, das für die Integration mit der Public-Key-Infrastruktur verwendet werden soll.

5. Geben Sie im Feld **Kennwort** das Domänenkennwort des Benutzerkontos an.

6. Wählen Sie in der Liste **Geben Sie den Namen der Zertifikatsvorlage im PKI-System an** die Zertifikatsvorlage aus, auf deren Grundlage die Zertifikate für die Domain-Benutzer ausgestellt werden.

   Unter diesem Benutzerkonto wird in Kaspersky Security Center ein Spezialdienst gestartet, der für die Ausstellung von Domänenzertifikaten der Benutzer verantwortlich ist. Der Dienst wird gestartet, wenn die Liste der Zertifikatsvorlagen mithilfe der Schaltfläche **Liste aktualisieren** heruntergeladen wird, oder wenn ein Zertifikat ausgestellt wird.

7. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

Die Integration der Zertifikatausstellung erfolgt daraufhin automatisch.

Unterstützung von Kerberos Constrained Delegation aktivieren

Das Programm unterstützt die Verwendung von Kerberos Constrained Delegation.

Um die Unterstützung von Kerberos Constrained Delegation zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten**.
2. Wählen Sie im Ordner **Mobile Geräte verwalten** den Unterordner **Server für mobile Geräte** aus.
3. Wählen Sie im Arbeitsplatz des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.
5. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Einstellungen** aus.
6. Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Kompatibilität mit Kerberos Constrained Delegation gewährleisten**.
7. Klicken Sie auf die Schaltfläche **OK**.

Mobiles Gerät zur Liste der verwalteten Geräte hinzufügen

Um ein mobiles Gerät des Benutzers zur Liste der verwalteten Geräte hinzuzufügen, muss auf dem Gerät ein allgemeines Zertifikat hinzugefügt und installiert werden. Allgemeine Zertifikate werden für die Identifizierung von mobilen Geräten durch den Administrationsserver verwendet. Nach der Zustellung und Installation eines allgemeinen Zertifikats auf dem mobilen Gerät wird dieses in der Liste der verwalteten Geräte angezeigt. Das Hinzufügen von mobilen Geräten der Benutzer zur Liste der verwalteten Geräte erfolgt mithilfe des Assistenten.

Assistent für das Hinzufügen neuer Geräte starten

Um den Assistenten für das Hinzufügen von mobilen Geräten zu starten, 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 **Mobiles Gerät hinzufügen** aus.

   Der Assistent für das Hinzufügen von mobilen Geräten wird gestartet.

4. Wählen Sie im Fenster **Betriebssystem** den Typ des Betriebssystems des mobilen Geräts (*Android*, *iOS*) aus.

Ihre weiteren Aktionen im Assistenten für das Hinzufügen von mobilen Geräten hängen davon ab, welchen Betriebssystem-Typ des mobilen Geräts Sie ausgewählt haben (s. Anweisungen unten).

Mobiles Gerät hinzufügen, wenn das allgemeine Zertifikat mithilfe eines Links zum App Store zugestellt wird

Gehen Sie wie folgt vor, um auf dem iOS-Gerät die App Kaspersky Safe Browser aus dem App Store zu installieren und anschließend das Gerät mit dem Administrationsserver zu verbinden:

1. Im Fenster des Assistenten **Betriebssystem** wählen Sie als Typ des Betriebssystems des mobilen Geräts **iOS** aus.

2. Wählen Sie im Fenster des Assistenten **Schutzmethode des iOS MDM-Geräts** die Option **Kaspersky Safe Browser über den Link aus dem AppStore installieren**.

3. 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 mobilen Gerät hinzufügen.
    - Die Datei des allgemeinen Zertifikats angeben.

4. 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.

5. Klicken Sie im Fenster **Ergebnis** 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 mobile Gerät des Benutzers gesendet. Der Benutzer klickt auf den Link oder scannt den QR-Code. Daraufhin zeigt das Betriebssystem des mobilen Geräts 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. Danach muss auf dem mobilen Gerät ein allgemeines Zertifikat (s. Abschnitt "Zertifikat installieren" auf S. 277) installiert werden. In diesem Fall wird Kaspersky Safe Browser nicht heruntergeladen und nicht installiert.

Mobiles Gerät hinzufügen, wenn das allgemeine Zertifikat als Teil des iOS MDM-Profils zugestellt wird

Um ein iOS-Gerät über das iOS MDM-Protokoll mit dem Administrationsserver zu verbinden, gehen Sie wie folgt vor:

1. Im Fenster des Assistenten **Betriebssystem** wählen Sie als Typ des Betriebssystems des mobilen Geräts **iOS** aus.

2. Wählen Sie im Fenster des Assistenten **Schutzmethode des iOS MDM-Geräts** die Variante **iOS MDM-Profil des iOS MDM-Servers verwenden** aus.

   Wählen Sie im nächsten Feld den iOS MDM-Server aus.

3. 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 mobilen Gerät hinzufügen.
   - Die Datei des allgemeinen Zertifikats angeben.

4. 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.

5. Klicken Sie im Fenster **Ergebnis** auf die Schaltfläche **Fertig**, um den Assistent zum Erstellen eines neuen Zertifikats zu beenden.

Daraufhin wird das iOS MDM-Profil automatisch auf dem Webserver von Kaspersky Security Center veröffentlicht. Der Benutzer des mobilen Geräts erhält eine Benachrichtigung mit dem Link zum Herunterladen des iOS MDM-Profils vom Webserver. Der Benutzer soll auf den empfangenen Link klicken. Daraufhin zeigt das Betriebssystem des mobilen Geräts dem Benutzer eine Zustimmungsaufforderung zur Installation des iOS MDM-Profils an. Stimmt der Benutzer zu, wird das iOS MDM-Profil auf das mobile

Gerät heruntergeladen. Nach dem Herunterladen des iOS MDM-Profils und der Synchronisierung mit dem Administrationsserver wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

> Damit der Benutzer über den erhaltenen Link auf den Webserver von Kaspersky Security Center wechseln kann, ist es erforderlich, dass sein mobiles Gerät auf die Verbindung mit dem Administrationsserver über den Port 8061 zugreifen kann.

Mobiles Gerät hinzufügen, wenn das allgemeine Zertifikat mithilfe eines Links zu Google Play zugestellt wird

Um auf dem KES-Gerät die App Kaspersky Endpoint Security für Android aus Google Play zu installieren und anschließend das Gerät mit dem Administrationsserver zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie im Fenster des Assistenten **Betriebssystem** als Typ des Betriebssystems des mobilen Geräts **Android** aus.

2. Wählen Sie im Fenster des Assistenten **Installationsmethode für Kaspersky Endpoint Security für Android** die Option **Über einen Link zu Google Play** aus.

3. 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 mobilen Gerät hinzufügen.
   - Die Datei des allgemeinen Zertifikats angeben.

4. 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.

5. Klicken Sie im Fenster **Ergebnis** 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 an das mobile Gerät des Benutzers gesendet. Der Benutzer klickt auf den Link oder scannt den QR-Code. Daraufhin zeigt das Betriebssystem des mobilen Geräts 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.

Mobiles Gerät hinzufügen, wenn das allgemeine Zertifikat als Teil der mobilen App zugestellt wird

Um auf dem Android-Gerät die App Kaspersky Endpoint Security für Android für mobile Geräte zu installieren und anschließend das Gerät mit dem Administrationsserver zu verbinden, gehen Sie wie folgt vor:

Für die Installation wird die auf dem Administrationsserver veröffentlichte App Kaspersky Security für mobile Endgeräte verwendet.

1. Wählen Sie im Fenster des Assistenten **Betriebssystem** als Typ des Betriebssystems des mobilen Geräts **Android** aus.

2. Wählen Sie im Fenster des Assistenten **Installationsmethode für Kaspersky Endpoint Security für Android** die Option **Über einen Link zu Ihrem Webserver** aus.

   Wählen Sie im folgenden Feld ein Installationspaket aus oder erstellen Sie ein neues Installationspaket über die Schaltfläche **Neu**.

3. 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 mobilen Gerät hinzufügen.
    - Die Datei des allgemeinen Zertifikats angeben.

4. 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.

5. Klicken Sie im Fenster **Ergebnis** auf die Schaltfläche **Fertig**, um den Assistent zum Erstellen eines neuen Zertifikats zu beenden.

Daraufhin wird das Paket für mobile Anwendungen für Kaspersky Endpoint Security für Android-Geräte automatisch auf dem Webserver von Kaspersky Security Center veröffentlicht. Das Paket für mobile Apps enthält die App, die Verbindungseinstellungen des mobilen Geräts für den Administrationsserver und das Zertifikat. Der Benutzer des mobilen Geräts erhält eine Benachrichtigung mit dem Link zum Herunterladen des Pakets vom Webserver. Der Benutzer soll auf den empfangenen Link klicken. Daraufhin zeigt das Betriebssystem dem Benutzer eine Zustimmungsaufforderung zur Installation des Pakets für mobile Apps an. Stimmt der Benutzer zu, wird das Paket auf das mobile Gerät heruntergeladen. Nach dem Herunterladen des Pakets und der Synchronisierung mit dem Administrationsserver wird das mobile Gerät im Unterordner **Mobile Geräte** des Ordners **Mobile Geräte verwalten** der Konsolenstruktur angezeigt.

Exchange ActiveSync-Mobilgeräte verwalten

In diesem Abschnitt werden die zusätzlichen Möglichkeiten zur Verwaltung von EAS-Geräten mithilfe von Kaspersky Security Center beschrieben.

Außer der Verwaltung von EAS-Geräten mithilfe von Befehlen hat der Administrator folgende Möglichkeiten:

- Profile zur Verwaltung von EAS-Geräten erstellen und ihnen Postfächer der Benutzer zuweisen (s. S 290). Bei einem *Profil zur Verwaltung von EAS-Geräten* handelt es sich um eine Exchange ActiveSync-Richtlinie, die für die Verwaltung von EAS-Geräten auf dem Microsoft Exchange Server verwendet wird. Im Profil zur Verwaltung von EAS-Geräten können Sie folgende Einstellungsgruppen anpassen:
  - Einstellungen zur Verwaltung von Benutzerkennwörtern.
  - E-Mail-Synchronisierungseinstellungen.
  - Beschränkungen für die Nutzung der Funktionen des mobilen Geräts.
  - Beschränkungen für die Nutzung von Apps auf dem mobilen Gerät.

  > Abhängig vom Modell des mobilen Geräts können die Einstellungen des Verwaltungsprofils eventuell nur zum Teil angewendet werden.
  > Der Anwendungsstatus der Exchange ActiveSync-Richtlinie kann in den Eigenschaften des mobilen Geräts angezeigt werden.

- Informationen über die Verwaltungseinstellungen für EAS-Geräte anzeigen (s. S 293). Beispielsweise kann der Administrator in den Eigenschaften des mobilen Geräts den Zeitpunkt der letzten Synchronisierung des mobilen Geräts mit dem Microsoft Exchange Server, die ID des EAS-Gerätes, den Namen der Exchange ActiveSync-Richtlinie und den Status ihrer Anwendung auf dem Gerät ablesen.

- Vom Benutzer nicht verwendete EAS-Geräte von der Verwaltung ausschließen (s. S. 293).

- Einstellungen für die Abfrage des Active Directory durch den Exchange ActiveSync-Server für mobile Geräte anpassen, auf deren Grundlage die Informationen über die Postfächer der Benutzer und ihre mobilen Geräte aktualisiert werden.

Sie können Informationen zur Verbindung von Exchange ActiveSync-Mobilgeräten mit dem Exchange ActiveSync-Server für mobile Geräte dem *Kaspersky Security Center Implementierungshandbuch* entnehmen.

Verwaltungsprofil hinzufügen

Sie können zu Verwaltung von EAS-Geräten Profile zur Verwaltung von EAS-Geräten erstellen und ihnen ausgewählte Microsoft Exchange-Postfächer zuweisen.

> Einem Microsoft Exchange-Postfach kann nur ein Verwaltungsprofil für EAS-Geräte zugewiesen werden.

Um ein Verwaltungsprofil für EAS-Geräte für das Microsoft Exchange-Postfach hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten**.

2. Wählen Sie im Ordner **Mobile Geräte verwalten** den Unterordner **Server für mobile Geräte** aus.

3. Wählen Sie im Arbeitsplatz des Ordners **Server für mobile Geräte** Exchange ActiveSync-Server für mobile Geräte aus.

4. Klicken Sie mit der rechten Maustaste auf den Exchange ActiveSync-Server für mobile Geräte und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Servers für mobile Geräte wird geöffnet.

5. Wählen Sie im Eigenschaftenfenster **des Exchange ActiveSync-Servers für mobile Geräte** den Abschnitt **E-Mail Postfächer** aus.

6. Wählen Sie ein Postfach aus und klicken Sie auf die Schaltfläche **Profil bestimmen**.

   Das Fenster **Richtlinienprofile** wird geöffnet.

7. Klicken Sie im Fenster **Richtlinienprofile** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Neues Profil** wird geöffnet.

8. Konfigurieren Sie die Profileinstellungen auf den Registerkarten des Fensters **Neues Profil**.

   - Wenn Sie den Namen des Profils und die Häufigkeit seiner Aktualisierung angeben möchten, wählen Sie die Registerkarte **Allgemein**.
   - Wenn Sie die Kennworteinstellungen für den Benutzer des mobilen Geräts anpassen möchten, wählen Sie die Registerkarte **Kennwort**.
   - Wenn Sie die Synchronisierungseinstellungen mit dem Microsoft Exchange Server anpassen möchten, wählen Sie die Registerkarte **Synchronisierungs-Einstellungen**.
   - Wenn Sie die Einstellungen für die Beschränkung der Funktionen des mobilen Geräts anpassen möchten, wählen Sie die Registerkarte **Gerät**.
   - Wenn Sie die Einstellungen für die Beschränkung der Nutzung von mobilen Apps auf dem mobilen Gerät anpassen möchten, wählen Sie die Registerkarte **Apps für das Gerät**.

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

   Das neue Profil wird in der Profilliste im Fenster **Richtlinienprofile** angezeigt.

   Wenn Sie möchten, dass dieses Profil einem neuen Postfach sowie einem Postfach, dessen Profil gelöscht wurde, automatisch zugewiesen wird, wählen Sie es in der Profilliste aus und klicken Sie auf die Schaltfläche **Als Standardprofil verwenden**.

   > Das Standardprofil kann nicht gelöscht werden. Um das aktuelle Standardprofil zu löschen, ist es erforderlich, ein anderes Profil als Standardprofil auszustellen.

10. Klicken Sie im Fenster **Richtlinienprofile** auf die Schaltfläche **OK**.

    Die Einstellungen des Verwaltungsprofils werden bei der nächsten Synchronisierung des Geräts mit dem Exchange ActiveSync-Server für mobile Geräte auf das EAS-Gerät angewendet.

Verwaltungsprofil löschen

Um ein Verwaltungsprofil für EAS-Geräte für das Microsoft Exchange-Postfach zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten**.

2. Wählen Sie im Ordner **Mobile Geräte verwalten** den Unterordner **Server für mobile Geräte** aus.

3. Wählen Sie im Arbeitsplatz des Ordners **Server für mobile Geräte** Exchange ActiveSync-Server für mobile Geräte aus.

4. Klicken Sie mit der rechten Maustaste auf den Exchange ActiveSync-Server für mobile Geräte und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Servers für mobile Geräte wird geöffnet.

5. Wählen Sie im Eigenschaftenfenster des Exchange ActiveSync-Servers für mobile Geräte den Abschnitt **E-Mail Postfächer** aus.

6. Wählen Sie ein Postfach aus und klicken Sie auf die Schaltfläche **Profile ändern**.

   Das Fenster **Richtlinienprofile** wird geöffnet.

7. Wählen Sie im Fenster **Richtlinienprofile** das Profil aus, das Sie löschen möchten, und klicken Sie auf die durch ein rotes Kreuz gekennzeichnete Schaltfläche zum Löschen.

   Das ausgewählte Profil wird aus der Liste der Verwaltungsprofile gelöscht. Für EAS-Geräte, die vom gelöschten Profil verwaltet wurden, wird das aktuelle Standardprofil angewendet.

   > Wenn Sie das aktuelle Standardprofil entfernen möchten, weisen Sie die Eigenschaft "Standardprofil" einem anderen Profil zu und entfernen Sie dann das Profil.

Informationen über das EAS-Gerät anzeigen

Gehen Sie folgendermaßen vor, um Informationen über ein EAS-Gerät anzuzeigen:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die EAS-Geräte im Arbeitsplatz nach Typ des Verwaltungsprotokolls (*EAS*).

3. Klicken Sie mit der rechten Maustaste auf das gewünschte mobile Gerät und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster des EAS-Geräts geöffnet.

Im Eigenschaftenfenster des mobilen Geräts werden Informationen über das angeschlossene EAS-Gerät angezeigt.

Ausschluss eines EAS-Geräts von der Verwaltung

Um ein EAS-Gerät von der Verwaltung durch den Exchange ActiveSync-Server für mobile Geräte auszuschließen, gehen Sie folgendermaßen vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die EAS-Geräte im Arbeitsplatz nach Typ des Verwaltungsprotokolls (*EAS*).

3. Wählen Sie das mobile Gerät, das Sie aus der Verwaltung durch den Exchange ActiveSync-Server für mobile Geräte nehmen möchten.

4. Wählen Sie im Kontextmenü des mobilen Geräts den Punkt **Entfernen**.

Daraufhin wird das EAS-Gerät durch ein Symbol mit einem roten Kreuz zum Löschen markiert. Das tatsächliche Löschen des Geräts aus der Liste der verwalteten Geräte erfolgt, nachdem es aus den Datenbanken des Exchange ActiveSync-Servers für mobile Geräte gelöscht wurde. Dazu muss der Administrator das Benutzerkonto des Benutzers auf dem Microsoft Exchange-Server löschen.

Verwaltung der iOS MDM-Geräte

In diesem Abschnitt werden die zusätzlichen Möglichkeiten zur Verwaltung von iOS MDM-Geräten mithilfe von Kaspersky Security Center beschrieben. Das Programm bietet folgende Möglichkeiten zur Verwaltung von iOS MDM-Geräten:

- Einstellungen für die verwalteten iOS MDM-Geräte zentral anpassen und die Funktionen der Geräte mithilfe von Konfigurationsprofilen beschränken. Sie können Konfigurationsprofile hinzufügen und ändern sowie Profile auf mobilen Geräten installieren.
- Apps mithilfe von Provisioning-Profilen nicht über den App Store auf mobilen Geräten installieren. Beispielsweise können Sie mithilfe von Provisioning-Profilen firmenintern entwickelte Unternehmens-Apps auf den mobilen Geräten der Benutzer installieren. Ein Provisioning-Profil enthält Informationen über die App und das mobile Gerät.
- Apps auf dem iOS MDM-Gerät über den App Store installieren. Vor der Installation der App auf dem iOS MDM-Gerät muss die App zum iOS MDM-Server hinzugefügt werden.

Sämtliche verbundenen iOS MDM-Geräte erhalten alle 24 Stunden PUSH-Benachrichtigungen zur Synchronisierung der Daten mit dem iOS MDM-Server.

> Die Informationen zur Installation des iOS MDM-Servers können Sie dem *Kaspersky Security Center Implementierungshandbuch* entnehmen.

Die Informationen über das Konfigurationsprofil und das Provisioning-Profil sowie über die auf dem iOS MDM-Gerät installierten Anwendungen können im Fenster Geräteeigenschaften angezeigt werden (s. Abschnitt "Informationen über das iOS MDM-Gerät anzeigen" auf S. 309).

Zertifikat für iOS MDM-Profil ausstellen

Sie können ein Zertifikat für ein iOS MDM-Profil ausstellen, mit dem dessen Authentizität durch das mobile Gerät bestimmt werden kann.

Um ein Zertifikat für ein iOS MDM-Profil zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Der Ordner **Mobile Geräte verwalten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Klicken Sie mit der rechten Maustaste auf den Ordner **Mobile Geräte** und wählen Sie den Punkt **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Ordners den Abschnitt **Verbindungseinstellungen für iOS-Geräte**.

4. Klicken Sie auf die Schaltfläche **Festlegen** neben dem Feld **Wählen Sie ein Zertifikat aus**.

   Daraufhin öffnet sich das Fenster **Zertifikat**.

5. Wählen Sie im Feld **Zertifikatstyp** entweder einen offenen oder geschlossenen Zertifikatstyp aus.

   - Wenn der Wert **Container PKCS#12** ausgewählt ist, geben Sie die Zertifikatsdatei und das Kennwort an.

   - Wenn der Wert **X.509-Zertifikat** ausgewählt ist:

     a. Geben Sie die Datei des privaten Schlüssels an (Datei mit der Erweiterung *prk oder *.pem).

     b. Geben Sie das Kennwort des privaten Schlüssels an.

     c. Geben Sie die Datei des offenen Schlüssels an (Datei mit der Erweiterung *.cer).

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

Daraufhin wird ein Zertifikat für das iOS MDM-Profil ausgestellt.

Konfigurationsprofil hinzufügen

Um ein Konfigurationsprofil zu erstellen, muss auf dem Gerät, auf dem sich die Verwaltungskonsole befindet, die iPhone Configuration Utility installiert sein. Das Programm iPhone Configuration Utility wird von der Apple-Webseite heruntergeladen und mithilfe der Standard-Tools des Betriebssystems installiert.

Um ein Konfigurationsprofil zu erstellen und es zum iOS MDM-Server hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten**.

   Der Ordner **Mobile Geräte verwalten** befindet sich standardmäßig im Ordner **Erweitert**.

2. Wählen Sie im Arbeitsplatz des Ordners **Mobile Geräte verwalten** den Unterordner **Server für mobile Geräte** aus.

3. Wählen Sie im Arbeitsplatz des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.

4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Servers für mobile Geräte wird geöffnet.

5. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Konfigurationsprofile** aus.

6. Klicken Sie im Abschnitt **Konfigurationsprofile** auf die Schaltfläche **Erstellen**.

   Es öffnet sich das Fenster **Neues Konfigurationsprofil hinzufügen**.

7. Geben Sie im Fenster **Neues Konfigurationsprofil hinzufügen** den Namen des Profils sowie die ID des Profils an.

   Die Kennung des Konfigurationsprofils muss eindeutig sein. Der ID-Wert muss im Format Reverse-DNS angegeben werden (z. B. *com.companyname.identifier*).

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

   Das Programm iPhone Configuration Utility wird gestartet.

9. Passen Sie die Einstellungen des Profils mit dem Programm iPhone Configuration Utility an.

   Eine Beschreibung der Profileinstellungen und eine Konfigurationsanleitung finden Sie in der Dokumentation zum Programm iPhone Configuration Utility.

Nachdem das Profil mit dem Programm iPhone Configuration Utility angepasst wurde, erscheint das neue Konfigurationsprofil im Abschnitt **Konfigurationsprofile** des Eigenschaftenfensters für den iOS MDM-Server.

Das Konfigurationsprofil kann mithilfe der Schaltfläche **Ändern** bearbeitet werden.

Mithilfe der Schaltfläche **Importieren** können Sie ein Konfigurationsprofil ins Programm laden.

Konfigurationsprofile können mithilfe der Schaltfläche **Exportieren** in einer Datei gespeichert werden.

Das erstellte Profil muss auf den iOS MDM-Geräten installiert werden (s. Abschnitt "Konfigurationsprofil auf dem Gerät hinzufügen" auf S. 297).

Konfigurationsprofil auf dem Gerät hinzufügen

Gehen Sie wie folgt vor, um ein Konfigurationsprofil auf einem mobilen Gerät zu installieren:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, auf dem das Konfigurationsprofil installiert werden soll.

Sie können mehrere mobile Geräte auswählen und das Profil gleichzeitig darauf installieren.

4. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

5. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **Profil installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Profil installieren** auswählen.

   Daraufhin wird das Fenster **Profile auswählen** mit der Profilliste geöffnet. Wählen Sie aus der Liste das Profil aus, das auf dem mobilen Gerät installiert werden soll. Sie können gleichzeitig mehrere Profile auswählen und auf dem mobilen Gerät installieren. Verwenden Sie die Taste **UMSCHALT**, um einen Bereich von mehreren Profilen auszuwählen. Um mehrere einzelne Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **STRG**.

6. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Konfigurationsprofil auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Ausgeführt*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

7. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle für die Verwaltung des Mobilgeräts** zu schließen.

Das installierte Profil kann angezeigt und erforderlichenfalls gelöscht werden (s. Abschnitt "Konfigurationsprofil vom Gerät löschen" auf S. 299).

Konfigurationsprofil vom Gerät löschen

Um ein Konfigurationsprofil von einem mobilen Gerät zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz mithilfe des Links **iOS MDM**.

3. Wählen Sie das mobile Gerät des Benutzers, von dem das Konfigurationsprofil gelöscht werden soll.

   Sie können mehrere mobile Geräte auswählen und das Profil gleichzeitig von diesen Geräten löschen.

4. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

5. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **Profil entfernen** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können auch einen Befehl an das mobile Gerät senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Profil entfernen** auswählen.

   Daraufhin wird das Fenster **Profile entfernen** mit der Profilliste geöffnet.

6. Wählen Sie aus der Liste das Profil aus, das vom mobilen Gerät gelöscht werden soll. Sie können gleichzeitig mehrere Profile auswählen und vom mobilen Gerät löschen. Verwenden Sie die Taste **UMSCHALT**, um einen Bereich von mehreren Profilen auszuwählen. Um mehrere einzelne Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **STRG**.

7. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Konfigurationsprofil vom mobilen Gerät des Benutzers gelöscht. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

8. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung von mobilen Geräten** zu schließen.

Provisioning-Profil hinzufügen

Gehen Sie wie folgt vor, um ein Provisioning-Profil zum iOS MDM-Server hinzuzufügen:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten**.
2. Wählen Sie im Ordner **Mobile Geräte verwalten** den Unterordner **Server für mobile Geräte** aus.
3. Wählen Sie im Arbeitsplatz des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des Servers für mobile Geräte wird geöffnet.
5. Wechseln Sie im Eigenschaftenfenster **des iOS MDM-Servers** zum Abschnitt **Provisioning-Profile**.
6. Klicken Sie im Abschnitt **Provisioning-Profile** auf die Schaltfläche **Importieren** und geben Sie den Pfad zur Datei des Provisioning-Profils an.

Das Profil wird zu den Einstellungen des iOS MDM-Servers hinzugefügt.

Provisioning-Profile können mithilfe der Schaltfläche **Exportieren** in einer Datei gespeichert werden.

Das importierte Provisioning-Profil kann auf den iOS MDM-Geräten installiert werden (s. Abschnitt "Provisioning-Profil auf dem Gerät installieren" auf S. 301).

Provisioning-Profil auf dem Gerät installieren

Gehen Sie wie folgt vor, um ein Provisioning-Profil auf einem mobilen Gerät zu installieren:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, auf dem das Provisioning-Profil installiert werden soll.

   Sie können mehrere mobile Geräte auswählen und das Provisioning-Profil gleichzeitig darauf installieren.

4. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

5. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **Provisioning-Profil installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Provisioning-Profil installieren** auswählen.

   Daraufhin wird das Fenster **Provisioning-Profile auswählen** mit der Liste der Provisioning-Profile geöffnet. Wählen Sie aus der Liste das Provisioning-Profil aus, das auf dem mobilen Gerät installiert werden soll. Sie können gleichzeitig mehrere Provisioning-Profile auswählen und auf dem mobilen Gerät installieren. Verwenden Sie die Taste **UMSCHALT**, um einen Bereich von mehreren Provisioning-Profilen auszuwählen. Um mehrere einzelne Provisioning-Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **STRG**.

6. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Provisioning-Profil auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

7. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle für die Verwaltung des Mobilgeräts** zu schließen.

Das installierte Profil kann angezeigt und erforderlichenfalls gelöscht werden (s. Abschnitt "Provisioning-Profil vom Gerät löschen" auf S. 302).

Provisioning-Profil vom Gerät löschen

Um ein Provisioning-Profil von einem mobilen Gerät zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, von dem das Provisioning-Profil gelöscht werden soll.

   Sie können mehrere mobile Geräte auswählen und das Provisioning-Profil gleichzeitig von diesen Geräten löschen.

4. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

5. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **Provisioning-Profil löschen** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können auch einen Befehl an das mobile Gerät senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **Provisioning-Profil löschen** auswählen.

   Daraufhin wird das Fenster **Provisioning-Profile entfernen** mit der Profilliste geöffnet.

6. Wählen Sie aus der Liste das Provisioning-Profil aus, das vom mobilen Gerät gelöscht werden soll. Sie können gleichzeitig mehrere Provisioning-Profile auswählen und vom mobilen Gerät löschen. Verwenden Sie die Taste **UMSCHALT**, um einen Bereich von mehreren Provisioning-Profilen auszuwählen. Um mehrere einzelne Provisioning-Profile zu einer Gruppe zusammenzufügen verwenden Sie die Taste **STRG**.

7. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird das ausgewählte Provisioning-Profil vom mobilen Gerät des Benutzers gelöscht. Apps, die mit dem gelöschten Provisioning-Profil verknüpft sind, funktionieren dann nicht mehr. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

8. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung von mobilen Geräten** zu schließen.

Verwaltete Apps hinzufügen

Vor der Installation der App auf dem iOS MDM-Gerät muss die App zum iOS MDM-Server hinzugefügt werden. Eine App wird verwaltet, wenn sie mithilfe von Kaspersky Security Center auf dem Gerät installiert wurde. Eine verwaltete App kann mithilfe von Kaspersky Security Center ferngesteuert verwaltet werden.

Gehen Sie wie folgt vor, um eine verwaltete App zum iOS MDM-Server hinzuzufügen:

1. Öffnen Sie in der Konsolenstruktur den Ordner **Mobile Geräte verwalten**.
2. Wählen Sie im Ordner **Mobile Geräte verwalten** den Unterordner **Server für mobile Geräte** aus.
3. Wählen Sie im Arbeitsplatz des Ordners **Server für mobile Geräte** einen iOS MDM-Server aus.
4. Klicken Sie mit der rechten Maustaste auf den iOS MDM-Server und wählen Sie **Eigenschaften** aus.

   Das Eigenschaftenfenster des iOS MDM-Servers wird geöffnet.
5. Wählen Sie im Eigenschaftenfenster des iOS MDM-Servers den Abschnitt **Verwaltete Apps** aus.
6. Klicken Sie im Abschnitt **Verwaltete Apps** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **App hinzufügen** wird geöffnet.
7. Geben Sie im Fenster **App hinzufügen** im Feld **App-Name** den Namen der hinzugefügten App ein.
8. Geben Sie im Feld **Apple ID der Anwendung oder Link auf die Anwendung im App Store** die Apple ID der hinzugefügten App oder den Link zur Manifestdatei an, über den die App heruntergeladen werden kann.
9. Wenn Sie möchten, dass beim Löschen des iOS MDM-Profils gleichzeitig mit dem Profil auch die verwaltete App vom mobilen Gerät des Benutzers gelöscht wird, aktivieren Sie das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren**.

10. Wenn Sie ein Verschieben der App-Daten ins Backup mithilfe von iTunes verbieten möchten, aktivieren Sie das Kontrollkästchen **Erstellen von Sicherungskopien der Daten verbieten**.

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

Die hinzugefügte App wird im Abschnitt **Verwaltete Apps** des Eigenschaftenfensters des iOS MDM-Servers angezeigt.

App auf dem mobilen Gerät installieren

Gehen Sie wie folgt vor, um eine App auf einem mobilen iOS MDM-Gerät zu installieren:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Der Ordner **Mobile Geräte verwalten** befindet sich standardmäßig im Ordner **Erweitert**. Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Wählen Sie das iOS MDM-Gerät, auf dem die App installiert werden soll.

   Sie können mehrere mobile Geräte auswählen und die App gleichzeitig darauf installieren.

3. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

4. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **App installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **App installieren** auswählen.

   Daraufhin wird das Fenster **Apps zur Installation auswählen** mit einer Liste der Apps geöffnet. Wählen Sie aus der Liste die App aus, die auf dem mobilen Gerät installiert werden soll. Sie können gleichzeitig mehrere Apps auswählen und auf dem mobilen Gerät installieren. Verwenden Sie die Taste **UMSCHALT**, um einen Bereich von mehreren Apps auszuwählen. Um mehrere einzelne Apps zu einer Gruppe zusammenzufügen verwenden Sie die Taste **STRG**.

5. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird die ausgewählte App auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden. Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

6. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung von mobilen Geräten** zu schließen.

Informationen über die installierte App werden in den Eigenschaften des iOS MDM-Mobilgeräts angezeigt (s.Abschnitt "Informationen über das iOS MDM-Gerät anzeigen" auf S. 309).
Sie können eine App vom mobilen Gerät mithilfe des Befehlsberichts oder aus dem Kontextmenü des Geräts deinstallieren (s. Abschnitt "Anwendung vom Gerät löschen" auf S. 306).

App vom Gerät löschen

Um eine App von einem mobilen Gerät zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz anhand des Verwaltungsprotokolls *iOS MDM*.

3. Wählen Sie das mobile Gerät des Benutzers, von dem die App gelöscht werden soll.

Sie können mehrere mobile Geräte auswählen und die App gleichzeitig von diesen Geräten löschen.

4. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

5. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **App löschen** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das mobile Gerät auch senden, indem Sie im Kontextmenü des Geräts den Punkt **Alle Befehle** und dann **App löschen** auswählen.

   Daraufhin wird das Fenster **Apps entfernen** mit einer Liste der Anwendungen geöffnet.

6. Wählen Sie aus der Liste die App aus, die vom mobilen Gerät gelöscht werden soll.
   Sie können gleichzeitig mehrere Apps auswählen und vom Gerät löschen. Verwenden Sie die Taste **UMSCHALT**, um einen Bereich von mehreren Apps auszuwählen. Um mehrere einzelne Apps zu einer Gruppe zusammenzufügen verwenden Sie die Taste **STRG**.

7. Klicken Sie auf die Schaltfläche **OK**, um den Befehl an das mobile Gerät zu senden.

   Nachdem der Befehl ausgeführt wurde, wird die ausgewählte App vom mobilen Gerät des Benutzers gelöscht. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls auf *Beendet*.

   Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden.

   Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

   Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

8. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle zur Verwaltung von mobilen Geräten** zu schließen.

App Kaspersky Safe Browser auf einem mobilen Gerät installieren

Gehen Sie wie folgt vor, um die App Kaspersky Safe Browser auf einem mobilen iOS MDM-Gerät zu installieren:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Der Ordner **Mobile Geräte verwalten** befindet sich standardmäßig im Ordner **Erweitert**. Im Arbeitsplatz des Ordners **Mobile Geräte verwalten** wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Wählen Sie das iOS MDM-Gerät, auf dem die App Kaspersky Safe Browser installiert werden soll.

   Sie können mehrere mobile Geräte auswählen und die App Kaspersky Safe Browser gleichzeitig darauf installieren.

3. Wählen Sie im Kontextmenü des mobilen Geräts die Option **Befehlsprotokoll anzeigen**.

4. Wechseln Sie im Fenster **Befehle für die Verwaltung des Mobilgeräts** zum Abschnitt **Kaspersky Safe Browser installieren** und klicken Sie auf die Schaltfläche **Befehl senden**.

   Sie können einen Befehl an das Gerät auch senden, indem Sie im Kontextmenü des mobilen Geräts den Punkt **Alle Befehle** und dann **Kaspersky Safe Browser installieren** auswählen.

   Nachdem der Befehl ausgeführt wurde, wird die App Kaspersky Safe Browser auf dem mobilen Gerät des Benutzers installiert. Bei erfolgreicher Ausführung des Befehls ändert sich der Status des Befehls im Befehlsprotokoll auf *Beendet*.

Mithilfe der Schaltfläche **Erneut senden** kann der Befehl noch einmal an das mobile Gerät des Benutzers gesendet werden. Mithilfe der Schaltfläche **Aus Warteschlange löschen** kann die Ausführung des gesendeten Befehls storniert werden, sofern der Befehl noch nicht ausgeführt wurde.

Im Block **Befehlsprotokoll** werden die Befehle, die an das mobile Gerät gesendet wurden, sowie der Status ihrer Ausführung angezeigt. Mithilfe der Schaltfläche **Aktualisieren** können Sie die Befehlsliste aktualisieren.

5. Klicken Sie auf die Schaltfläche **OK**, um das Fenster **Befehle für die Verwaltung des Mobilgeräts** zu schließen.

Informationen über die installierte App Kaspersky Safe Browser werden in den Eigenschaften des iOS MDM-Mobilgeräts angezeigt (s.Abschnitt "Informationen über das iOS MDM-Gerät anzeigen" auf S. 309). Sie können eine App vom mobilen Gerät mithilfe des Befehlsberichts oder aus dem Kontextmenü des mobiles Geräts deinstallieren (s. Abschnitt "App vom Gerät löschen" auf S. 306).

Informationen über das iOS MDM-Gerät anzeigen

Gehen Sie folgendermaßen vor, um Informationen über ein iOS MDM-Gerät anzuzeigen:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz mithilfe des Links **iOS MDM**.

3. Wählen Sie das mobile Gerät, über das Informationen angezeigt werden sollen.

4. Klicken Sie mit der rechten Maustaste auf das gewünschte mobile Gerät und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Eigenschaftenfenster des iOS MDM-Geräts geöffnet.

Im Eigenschaftenfenster des mobilen Geräts werden Informationen über das angeschlossene iOS MDM-Gerät angezeigt.

Ausschluss eines iOS MDM-Geräts von der Verwaltung

Um ein iOS MDM-Gerät vom iOS MDM-Server auszuschließen, gehen Sie folgendermaßen vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die iOS MDM-Geräte im Arbeitsplatz mithilfe des Links **iOS MDM**.

3. Wählen Sie das mobile Gerät aus, das ausgeschlossen werden soll.

4. Wählen Sie im Kontextmenü des mobilen Geräts den Punkt **Entfernen**.

Daraufhin wird das iOS MDM-Gerät in der Liste zum Löschen markiert. Nachdem das mobile Gerät aus den Datenbanken des iOS MDM-Servers gelöscht wurde, wird es automatisch aus der Liste der verwalteten Geräte gelöscht. Für das Löschen des mobilen Geräts aus den Datenbanken des iOS MDM-Servers wird etwa eine Minute benötigt.

Als Folge des Ausschlusses eines iOS MDM-Geräts von der Verwaltung werden alle installierten Konfigurationsprofile, iOS MDM-Profile und Anwendungen, für die das Kontrollkästchen **Zusammen mit dem iOS MDM-Profil deinstallieren** aktiviert ist, vom Gerät gelöscht (s. Abschnitt "**Verwaltete Anwendung hinzufügen**" auf S. 304).

KES-Geräte verwalten

Kaspersky Security Center unterstützt folgende Möglichkeiten zur Verwaltung von mobilen KES-Geräten:

- KES-Geräte mithilfe von Befehlen zentral verwalten (s. Abschnitt "Befehle zur Verwaltung von mobilen Geräten" auf S. 270);
- Informationen über die Einstellungen für die Verwaltung von KES-Geräten anzeigen (s. Abschnitt "Informationen über das KES-Gerät anzeigen" auf S. 313);

- Apps mithilfe von Paketen für mobile Anwendungen installieren (s. Abschnitt "Paket für mobile Anwendungen für KES-Geräte erstellen" auf S. 311);
- KES-Geräte von der Verwaltung ausschließen (s. Abschnitt "Ausschluss eines KES-Geräts von der Verwaltung" auf S. 314).

Eine detaillierte Beschreibung der Arbeit mit KES-Geräten und Informationen zur Verbindung von KES-Geräten mit dem Administrationsserver finden Sie im *Implementierungshandbuch zu Kaspersky Security Center 10*.

Paket für mobile Apps für KES-Geräte erstellen

Für die Erstellung eines Pakets für mobile Apps ist für KES-Geräte eine Lizenz für Kaspersky Security 10 für mobile Endgeräte erforderlich.

Gehen Sie wie folgt vor, um ein Paket für mobile Apps zu erstellen:

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. Klicken Sie im Fenster **Pakete für mobile Anwendungen verwalten** auf die Schaltfläche **Neu**.

4. Der Assistent für die Erstellung eines Pakets für mobile Apps wird gestartet. Folgen Sie den Anweisungen des Assistenten.

5. Wenn Sie das Programm in einen Container ablegen möchten, aktivieren Sie im Fenster des Assistenten **Einstellungen** das Kontrollkästchen **Container mit ausgewähltem Programm erstellen**.

Das erstellte Paket für mobile Apps wird im Fenster **Pakete für mobile Apps verwalten** angezeigt.

Die Container werden zur Aktivitätskontrolle für Programme verwendet, die auf dem mobilen Gerät des Benutzers gestartet werden. Auf die im Container abgelegten Programme können die Regeln der Sicherheitsrichtlinie angewandt werden. Die Regeln für Programme können Sie im Eigenschaftenfenster der Richtlinie von Kaspersky Security 10 für mobile Endgeräte im Abschnitt **Container** anpassen. Ausführliche Informationen über Container und die Verwaltung von diesen können Sie den Dokumentationen zum Programm Kaspersky Security 10 für mobile Endgeräte entnehmen.

Der Container kann Programme von Drittanbietern enthalten. Das Programmpaket von Kaspersky Security 10 für mobile Endgeräte darf nicht in den Container abgelegt werden.

Zwei-Faktor-Authentifizierung von KES-Geräten aktivieren

Gehen Sie folgendermaßen vor, um die Zwei-Faktor-Authentifizierung des KES-Geräts zu aktivieren:

1. Öffnen Sie die Systemregistrierung des Client-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:

     HKLM\Software\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Erstellen Sie einen Schlüssel mit dem Namen LP_MobileMustUseTwoWayAuthOnPort13292.

4. Geben Sie als Schlüsseltyp REG_DWORD an.

5. Legen Sie den Wert des Schlüssels mit 1 fest.

6. Starten Sie den Dienst des Administrationsservers neu.

Daraufhin wird nach dem Start des Dienstes des Administrationsservers die verpflichtende Zwei-Faktor-Authentifizierung des KES-Geräts unter Verwendung des allgemeinen Zertifikats aktiviert.

> Bei der ersten Verbindung des KES-Geräts mit dem Administrationsserver muss das Zertifikat nicht verpflichtend vorhanden sein.

Die Zwei-Faktor-Authentifizierung von KES-Geräten ist standardmäßig deaktiviert.

Informationen über das KES-Gerät anzeigen

Gehen Sie folgendermaßen vor, um Informationen über ein KES-Gerät anzuzeigen:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die KES-Geräte im Arbeitsplatz nach dem Verwaltungsprotokoll *KES*.

3. Wählen Sie das mobile Gerät, dessen Informationen angezeigt werden sollen.

4. Klicken Sie mit der rechten Maustaste auf das gewünschte mobile Gerät und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Eigenschaftenfenster des KES-Geräts geöffnet.

Im Eigenschaftenfenster des mobilen Geräts werden Informationen über das angeschlossene KES-Gerät angezeigt.

Ausschluss eines KES-Geräts von der Verwaltung

Um ein KES-Gerät von der Verwaltung auszuschließen, muss der Benutzer den Administrationsagenten vom mobilen Gerät löschen. Nach dem Löschen des Administrationsagenten durch den Benutzer werden die Informationen über das mobile Gerät aus den Datenbanken des Administrationsservers gelöscht. Anschließend kann der Administrator das Gerät aus der Liste der verwalteten Geräte löschen.

Gehen Sie folgendermaßen vor, um ein KES-Gerät aus der Liste der verwalteten Geräte zu löschen:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** der Konsolenstruktur den Unterordner **Mobile Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der verwalteten mobilen Geräte angezeigt.

2. Filtern Sie die KES-Geräte im Arbeitsplatz nach dem Verwaltungsprotokoll *KES*.

3. Wählen Sie das mobile Gerät aus, das Sie aus der Verwaltung nehmen möchten.

4. Wählen Sie im Kontextmenü des mobilen Geräts den Punkt **Entfernen**.

Daraufhin wird das mobile Gerät aus der Liste der verwalteten Geräte gelöscht.

Wenn Kaspersky Endpoint Security für Android nicht vom mobilen Gerät gelöscht wird, erscheint das Gerät nach der Synchronisierung mit dem Administrationsserver wieder in der Liste der verwalteten Geräte.

Self Service Portal

Dieser Abschnitt enthält Informationen über das Self Service Portal. Sie finden hier Anleitungen zur Autorisierung von Benutzern auf dem Self Service Portal, zur Erstellung von Benutzerkonten für das Self Service Portal sowie zum Hinzufügen von mobilen Geräten auf dem Self Service Portal.

In diesem Abschnitt

Über das Self Service Portal

Das Self Service Portal ist ein Webportal, das dem Administrator erlaubt, den Benutzern einen Teil der Abläufe zur Verwaltung ihrer mobilen Geräte zu übertragen. Der Benutzer eines mobilen Geräts kann nach der Anmeldung auf dem Self Service Portal sein mobiles Gerät selbstständig zum Portal hinzufügen. Beim Hinzufügen des mobiles Geräts, wird auf das iOS MDM-Gerät ein iOS MDM-Profil installiert; auf die KES-Geräte wird Kaspersky Endpoint Security für Android installiert, und auf das Gerät werden Unternehmensrichtlinien angewandt (s. Abschnitt "Gerät hinzufügen" auf S. 318). Danach kann das mobile Gerät verwaltet werden.

Das Self Service Portal unterstützt die automatische Autorisierung von Benutzern mithilfe von Kerberos Constrained Delegation und die Domain-Autorisierung.

Das Self Service Portal unterstützt mobile Geräte mit den Betriebssystemen iOS und Android.

Der Benutzer kann im Self Service Portal folgende Aktionen ausführen:

- Apps aus dem App-Store des Unternehmens herunterladen. Die Apps müssen vorher in der Kaspersky Security Center 10 Web Console zum App-Store des Unternehmens hinzugefügt werden. Detaillierte Informationen über das Hinzufügen von Apps zum App-Store finden Sie im *Benutzerhandbuch für Kaspersky Security Center 10 Web Console*. Zum Herunterladen von Apps muss der Benutzer im Self Service Portal die Registerkarte **Apps** im Fenster Self Service Portal auswählen.

- Selbstständig Befehle an die verwalteten mobilen Geräte senden, z. B. bei Diebstahl oder Verlust des Geräts. Zum Versenden von Befehlen muss die Registerkarte **Geräte** im Fenster Self Service Portal ausgewählt werden. Für jeden Typ mobiler Geräte werden eigene Befehlssätze unterstützt (s. Tabelle unten).

- Das mobile Gerät selbständig über den Link **Entsperrungscode anzeigen** entsperren, wenn das Gerät gesperrt wurde.

Tabelle 3. Liste der unterstützten Befehle

Typ des mobilen Geräts	Befehle	Ergebnis der Befehlsausführung
iOS MDM-Gerät	Blockieren	Das mobile Gerät wurde gesperrt.
	Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen wurden auf Werkseinstellungen zurückgesetzt, das Gerät wird nicht mehr verwaltet.
	Unternehmensdaten löschen	Unternehmensdaten wurden gelöscht, das iOS MDM-Profil wurde gelöscht, der Administrationsagent wurde gelöscht, das mobile Gerät wird nicht mehr verwaltet.
KES-Gerät	Blockieren	Das mobile Gerät wurde gesperrt.
	Auf Werkseinstellungen zurücksetzen	Sämtliche Daten wurden vom mobilen Gerät gelöscht, die Einstellungen wurden auf Werkseinstellungen zurückgesetzt, das Gerät wird nicht mehr verwaltet.

Typ des mobilen Geräts	Befehle	Ergebnis der Befehlsausführung
	Unternehmensdaten löschen	Unternehmensdaten wurden gelöscht, das iOS MDM-Profil wurde gelöscht, der Administrationsagent wurde gelöscht, das mobile Gerät wird nicht mehr verwaltet.
	Standort ermitteln	Der Standort des mobilen Geräts wurde ermittelt und auf Google Maps angezeigt. Der Mobilfunkanbieter erhebt Gebühren für den SMS-Versand und die Verbindung mit dem Internet.
	Tonsignal wiedergeben	Das mobile Gerät gibt ein Tonsignal wieder.
	Bild aufnehmen	Das mobile Gerät wurde gesperrt. Mit der Frontkamera des mobilen Geräts wurde ein Foto aufgenommen und auf dem Administrationsserver gespeichert. Das Foto kann im Befehlsprotokoll auf dem Self Service Portal angezeigt werden. Der Mobilfunkanbieter erhebt Gebühren für den SMS-Versand und die Verbindung mit dem Internet.

Das Self Service Portal verwendet eine globale Liste der Benutzer von Kaspersky Security Center. Die Liste wird automatisch beim Import aus dem Active Directory (s. Abschnitt "Abfrageeinstellungen der Gruppe des Active Directory anzeigen und ändern" auf S. 213) oder manuell ergänzt (s. Abschnitt "Benutzerkonten hinzufügen" auf S. 180).

Wenn die Domain-Autorisierung auf dem Self Service Portal vom Administrator verboten wurde, können die Benutzer Anmeldenamen zur Autorisierung verwenden. Die Erstellung von Pseudonymen für die Autorisierung auf dem Self Service Portal erfolgt in den Eigenschaften der Benutzerkonten der Benutzer (s. Abschnitt "Benutzerkonto für das Self Service Portal erstellen" auf S. 319).

Der Administrator kann den Benutzern folgende Rechte für die Verwendung des Self Service Portals zuweisen:

- Lesen
- Ändern
- Neue Geräte verbinden
- Nur informative Befehle an mobile Geräte senden (die nicht den Zustand des Geräts ändern)

  Die Befehle **Bild aufnehmen** und **Standort ermitteln** sind informativ.
- Befehle an mobile Geräte senden.

Gerät hinzufügen

Vor dem Hinzufügen eines mobilen Geräts auf dem Self Service Portal muss der Benutzer den Lizenzvertrag für die Verwendung von Self Service Portal akzeptieren und sich auf dem Portal anmelden.

Der Algorithmus zum Hinzufügen eines mobilen Benutzergeräts auf dem Self Service Portal umfasst folgende Schritte:

1. Der Benutzer öffnet die Hauptseite des Portals.
2. Das Self Service Portal erstellt ein Installationspaket und zeigt danach einen Einmallink zum Download des Pakets und einen QR-Code an, in dem der Link enthalten ist. Auf dem Bildschirm wird angezeigt, wie lange der Link zum Herunterladen des Installationspakets noch verfügbar ist. Eine Nachricht mit dem Link zum Herunterladen des Installationspakets wird an die E-Mail-Adresse des Benutzers gesendet.

   Das Installationspaket ist für die Installation des Verwaltungsagenten auf dem mobilen Gerät und die Anwendung der Unternehmensrichtlinien erforderlich.

   > Ein neues Installationspaket kann nur erstellt werden, nachdem das vorher erstellte Paket vom Administrationsserver gelöscht wurde.

3. Mithilfe des Links **Paket für die Installation auf einem neuen Gerät erstellen** gelangt der Benutzer mit dem mobilen Gerät, das auf dem Self Service Portal hinzugefügt werden soll, auf die Downloadseite des Installationspakets.

4. Das Self Service Portal ermittelt das Betriebssystem des mobilen Benutzergeräts.

   Wenn das Betriebssystem des mobilen Geräts automatisch ermittelt werden konnte, wird die Downloadseite des Installationspakets geöffnet. Wenn das Betriebssystem nicht automatisch bestimmt werden konnte, wird ein Fenster zur manuellen Auswahl des Betriebssystems geöffnet.

5. Der Benutzer lädt das Installationspaket herunter und installiert den Verwaltungsassistenten auf dem mobilen Gerät.

6. Nach der Installation des Verwaltungsagenten wird das Gerät mit dem Administrationsserver verbunden.

Daraufhin wird das mobile Gerät zur Liste der verwalteten Geräte hinzugefügt, und die Unternehmensrichtlinien werden auf das Gerät angewandt. Der Link mit Informationen über die Verbindung zum Administrationsserver wird dem Benutzer per E-Mail zugestellt.

Benutzer mit dem Self Service Portal verbinden

Wenn die Verwendung der Domain-Autorisierung von Benutzern im Self Service Portal verboten ist, können Sie in der Verwaltungskonsole Anmeldenamen (alias accounts) für die Benutzer erstellen. Mithilfe der Anmeldenamen können die Benutzer eine Autorisierung auf dem Self Service Portal durchführen.

Um einen Benutzer (unter einem Anmeldenamen) mit dem Self Service Portal zu verbinden, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Mobile Geräte verwalten** den Unterordner **Self Service Portal**.

2. Klicken Sie im Arbeitsplatz des Ordners **Self Service Portal** auf die Schaltfläche **Einladung zur Verbindung mit dem Self Service Portal versenden**.

Daraufhin wird der Benutzer-Verbindungsassistent für das Self Service Portal gestartet. Folgen Sie den Schritten des Assistenten.

3. Im Fenster **Rechte anpassen** des Assistenten können Sie über den Link **Einstellungen** die Zugriffsrechte der Benutzer und Benutzergruppen zum Self Service Portal anpassen.

   Wenn das Kontrollkästchen **Diese Meldung nicht mehr anzeigen** aktiviert ist, wird beim folgenden Start des Assistenten das Fenster **Rechte anpassen** nicht angezeigt.

4. Im Fenster **Adresse des Self Service Portals auswählen** können Sie die Adresse des Self Service Portals angeben, an die der Benutzer angeschlossen wird.

   Sie können die Auswahl der Adresse des Self Service Portals überspringen. In diesem Fall muss im Text der Einladung die Adresse des Self Service Portals manuell angegeben werden.

5. Geben Sie im Fenster **Auswahl von Benutzern für die Verbindung mit dem Self Service Portal** die Benutzer an, die mit dem Self Service Portal verbunden werden sollen.

6. Passen Sie im Fenster **Anmeldenamen der Benutzerkonten anpassen** des Assistenten die Verwendung von Anmeldenamen und Domäneneinträgen der Benutzer für die Verbindung zum **Self Service Portal** an:

   - Aktivieren Sie das Kontrollkästchen **Anmeldenamen der Benutzerkonten für den Zugang zum Self Service Portal verwenden**, um den Versand von Einladungen für die Verbindung zum Self Service Portal an ausgewählte Benutzer anzupassen.

     Wenn das Kontrollkästchen deaktiviert ist, wird die Einladung für die Verbindung zum Self Service Portal nur an die im vorhergehenden Schritt des Assistenten ausgewählten Domänenbenutzer gesendet.

   - Wählen Sie die Option **Für Benutzer Anmeldenamen erstellen, falls nicht vorhanden**, damit Kaspersky Security Center für alle Benutzerkonten, die keinen Anmeldenamen haben, automatisch Namen erstellt. Die Einladungen für die Verbindung zum Self Service Portal werden an alle Benutzer gesendet, für die Anmeldenamen erstellt wurden. Kaspersky Security Center erstellt keine neuen Anmeldenamen für Benutzer, die bereits einen Anmeldenamen haben.

- Wählen Sie die Option **Benutzern ohne Anmeldenamen eine Einladung für ein Domänen-Benutzerkonto versenden**, damit das Programm für Domänenbenutzer, die keinen Anmeldenamen haben, nicht automatisch Namen erstellt. Falls der Benutzer keinen Anmeldenamen hat, wird die Einladung für die Verbindung zum Self Service Portal an den Domäneneintrag gesendet.

- Aktivieren Sie das Kontrollkästchen **Neue Kennwörter für Anmeldenamen erstellen**, damit Kaspersky Security Center für alle Anmeldenamen (für neue und früher erstellte) neue Kennwörter erstellt. Die Informationen über die neuen und alten Kennwörter werden den Benutzern im Text der Einladung für die Verbindung zum Self Service Portal zugesendet.

  Wenn das Kontrollkästchen deaktiviert ist, wird das Kennwort nur für die erneut erstellten Anmeldenamen generiert werden.

- In diesem Feld können Sie die Anzahl der Zeichen des Kennwortes für die Verbindung zum Self Service Portal für die Anmeldenamen der Benutzer festlegen. Die Länge des Kennwortes beträgt standardmäßig 16 Zeichen.

7. Wählen Sie im Fenster **Versand von Einladungen zu Self Service Portal** die Methode der Zustellung der Einladung zum Self Service Portal sowohl für neue als auch für existierende Benutzer.

8. Über den Link **Nachricht bearbeiten** können Sie den Text der Einladung anzeigen und erforderlichenfalls editieren.

Nach Abschluss des Assistenten erhalten die ausgewählten Benutzer eine Einladung mit Informationen für die Verbindung zum Self Service Portal. Für einen Benutzer kann eine unbegrenzte Anzahl von Anmeldenamen für das Self Service Portal erstellt werden. Nach dem Erstellen des Anmeldenamens wird er im Eigenschaftenfenster des Benutzerkontos im Abschnitt **Anmeldename des Benutzers für das Self Service Portal** angezeigt. Nach der Erstellung des Anmeldenamens des Benutzers für das Self Service Portal kann der Anmeldename nicht mehr geändert werden. Sie können den gewählten Anmeldenamen mithilfe der Schaltfläche mit dem roten Kreuz rechts neben der Liste der Anmeldenamen für das Self Service Portal löschen.

Verschlüsselung und Datenschutz

Die Datenverschlüsselung senkt das Risiko eines unbeabsichtigten Informationsverlustes im Falle des Diebstahls oder Verlustes eines tragbaren Geräts, eines Wechselmediums oder einer Festplatte, oder beim Zugriff nicht autorisierter Benutzer und Programme auf Daten.

Die Verschlüsselungsfunktion ist im Programm Kaspersky Endpoint Security 10 für Windows implementiert. Kaspersky Endpoint Security 10 für Windows ermöglicht die Verschlüsselung von Dateien, die auf den lokalen Festplatten eines Geräts oder auf Wechselmedien gespeichert sind, sowie die Verschlüsselung von ganzen Wechseldatenträgern und Festplatten.

Eine Konfiguration der Verschlüsselungsregeln erfolgt mit Kaspersky Security Center durch das Festlegen von Richtlinien. Die Verschlüsselung und Entschlüsselung nach den festgelegten Regeln erfolgen bei der Anwendung einer Richtlinie.

> Ob die Funktion zur Verschlüsselungsverwaltung verfügbar ist, wird durch die Einstellungen der Benutzeroberfläche definiert (s. Abschnitt "Benutzeroberfläche anpassen" auf S. 60).

Der Administrator kann folgende Aktionen ausführen:

- Verschlüsselung und Entschlüsselung von Dateien auf den lokalen Laufwerken eines Geräts anpassen
- Verschlüsselung und Entschlüsselung von Dateien auf Wechseldatenträgern anpassen
- Regeln für den Zugriff von Programmen auf verschlüsselte Dateien erstellen
- Schlüsseldatei für den Zugriff auf verschlüsselte Dateien erstellen und an den Benutzer weitergeben, wenn die Verschlüsselungsfunktion für Dateien auf dem Gerät des Benutzers beschränkt wurde
- Verschlüsselung von Festplatten anpassen und durchführen

- Zugriff von Benutzern auf verschlüsselte Festplatten und Wechseldatenträger verwalten (Benutzerkonten des Authentifizierungsagenten verwalten, Antworten auf Anfragen zum Wiederherstellen des Benutzernamens und -kennwortes sowie Zugriffsschlüssel auf verschlüsselte Geräte erstellen und an Benutzer weitergeben);

- Verschlüsselungsstatusmeldungen und Berichte über die Verschlüsselung von Dateien anzeigen.

Diese Vorgänge werden durch das Programm Kaspersky Endpoint Security 10 für Windows ausgeführt. Ausführliche Anweisungen zur Ausführung der Vorgänge und eine Beschreibung der Besonderheiten der Verschlüsselungsfunktion können Sie dem *Administratorhandbuch für Kaspersky Endpoint Security 10 für Windows* entnehmen.

In diesem Abschnitt

Liste der verschlüsselten Geräte anzeigen

Um sich eine Liste der Geräte anzeigen zu lassen, deren Informationen verschlüsselt wurden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur des Administrationsservers den Ordner **Verschlüsselung und Datenschutz** aus.

2. Wechseln Sie in die Liste der verschlüsselten Geräte auf eine der folgenden Weisen:

   - Klicken Sie im Block **Verschlüsselte Geräte verwalten** auf den Link **Zur Liste der verschlüsselten Geräte**.

   - Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselte Geräte** aus.

Daraufhin werden im Arbeitsplatz Informationen über die im Netzwerk vorhandenen Geräte, auf denen verschlüsselte Dateien vorhanden sind, angezeigt, sowie die Geräte, die auf der Ebene der Festplatten verschlüsselt wurden. Nachdem die Informationen auf einem Gerät entschlüsselt wurden, wird das Gerät automatisch aus der Liste entfernt.

Sie können die Informationen in der Geräteliste nach einer beliebigen Spalte in auf- oder absteigender Reihenfolge sortieren.

> Ob der Ordner **Verschlüsselung und Datenschutz** in der Konsolenstruktur angezeigt wird, wird durch die Einstellungen der Benutzeroberfläche definiert
> (s. Abschnitt "Benutzeroberfläche anpassen" auf S. 60).

Liste der Verschlüsselungsereignisse anzeigen

Bei der Ausführung der Aufgaben zur Datenverschlüsselung und -entschlüsselung auf den Client-Geräten sendet Kaspersky Endpoint Security 10 für Windows an Kaspersky Security Center Informationen über aufgetretene Ereignisse folgender Typen:

- Eine Datei kann nicht verschlüsselt oder entschlüsselt oder ein verschlüsseltes Archiv kann wegen zu wenig Speicherplatz auf der Festplatte nicht erstellt werden.
- Eine Datei kann nicht verschlüsselt oder entschlüsselt oder ein verschlüsseltes Archiv kann aufgrund eines Problems mit der Lizenz nicht erstellt werden.
- Eine Datei kann nicht verschlüsselt oder entschlüsselt oder ein verschlüsseltes Archiv kann wegen fehlender Zugriffsrechte nicht erstellt werden.
- Der Zugriff eines Programms auf eine verschlüsselte Datei wurde verweigert.
- Unbekannte Fehler.

Um sich eine Liste der Ereignisse anzeigen zu lassen, die bei einer Datenverschlüsselung auf Client-Geräten aufgetreten sind, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur des Administrationsservers den Ordner **Verschlüsselung und Datenschutz** aus.

2. Wechseln Sie in die Liste der Ereignisse, die bei der Datenverschlüsselung aufgetreten sind, auf eine der folgenden Weisen:

   - Klicken Sie im Verwaltungsblock **Fehler bei Datenverschlüsselung** auf den Link **Zur Fehlerliste**.

   - Wählen Sie in der Konsolenstruktur den Unterordner **Verschlüsselungsereignisse** aus.

Daraufhin werden im Arbeitsplatz Informationen über die Probleme angezeigt, die bei der Datenverschlüsselung auf den Client-Geräten aufgetreten sind.

Sie können folgende Aktionen auf die Liste der Verschlüsselungsereignisse anwenden:

- Einträge in jeder Spalte aufsteigend oder absteigend sortieren

- schnelle Suche nach Einträgen ausführen (nach einer Textübereinstimmung mit der Teilzeichenfolge in einem beliebigen Listenfeld)

- die erstellte Ereignisliste in eine Textdatei exportieren.

Ob der Ordner **Verschlüsselung und Datenschutz** in der Konsolenstruktur angezeigt wird, wird durch die Einstellungen der Benutzeroberfläche definiert (s. Abschnitt "Benutzeroberfläche anpassen" auf S. 60).

Liste der Verschlüsselungsereignisse in eine Textdatei exportieren

Um eine Liste der Verschlüsselungsereignisse in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Erstellen Sie eine Liste der Verschlüsselungsereignisse (s. Abschnitt "Liste der Verschlüsselungsereignisse anzeigen" auf S. 324).

2. Klicken Sie mit der rechten Maustaste auf die Ereignisliste und wählen Sie **Liste exportieren**.

   Das Fenster **Liste exportieren** wird geöffnet.

3. Geben Sie im Fenster **Liste exportieren** den Namen der Textdatei mit der Ereignisliste ein, wählen einen Ordner, in dem die Datei gespeichert werden soll, und klicken Sie auf die Schaltfläche **Speichern**.

   Die Liste der Verschlüsselungsereignisse wird in der angegebenen Datei gespeichert.

Verschlüsselungsberichte erstellen und anzeigen

Der Administrator kann folgende Berichte erstellen:

- Bericht über die Verschlüsselung von Massenspeichergeräten, in dem Informationen über den Verschlüsselungsstatus der Geräte für alle Gerätegruppen enthalten sind.

- Bericht über Zugriffsrechte auf verschlüsselte Geräte, in dem Informationen über den Status der Benutzerkonten enthalten sind, die Zugriff auf die verschlüsselten Geräte haben.

- Bericht über Fehler bei der Verschlüsselung von Dateien und Ordnern, in dem Informationen über Fehler enthalten sind, die bei der Ausführung der Aufgaben zur Datenverschlüsselung und -entschlüsselung auf den Client-Geräten aufgetreten sind.

- Bericht über den Verschlüsselungsstatus der verwalteten Geräte, in dem Informationen darüber enthalten sind, ob der Verschlüsselungsstatus der Geräte der Verschlüsselungsrichtlinie entspricht.

- Bericht über das Sperren des Zugriffs auf Dateien, in dem Informationen über das Sperren des Zugriffs von Apps auf verschlüsselte Dateien enthalten sind.

Um sich einen Bericht über die Verschlüsselung von Geräten anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselung und Datenschutz** aus.

2. Führen Sie eine der folgenden Aktionen aus:

   - Starten Sie durch Klicken auf den Link **Bericht über die Verschlüsselung von Geräten** den Assistenten für das Erstellen einer Berichtsvorlage.

   - Wählen Sie den Unterordner **Verschlüsselte Geräte** aus, und klicken Sie anschließend auf die Schaltfläche **Bericht über die Verschlüsselung von Geräten**, um den Assistenten für das Erstellen einer Berichtsvorlage zu starten.

3. Folgen Sie dem Assistenten für das Erstellen einer Berichtsvorlage.

Im Knoten **Administrationsserver** auf der Registerkarte **Berichte** wird ein neuer Bericht angezeigt. Der Vorgang zum Erstellen des Berichts wird gestartet. Der Bericht wird im Arbeitsplatz der Registerkarte **Berichte** angezeigt.

Um sich einen Bericht über die Zugriffsrechte auf verschlüsselte Geräte anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselung und Datenschutz** aus.

2. Führen Sie eine der folgenden Aktionen aus:

   - Starten Sie durch Klicken auf den Link **Bericht über Zugriffsrechte für verschlüsselte Geräte** im Block **Verschlüsselte Geräte verwalten** den Assistenten für das Erstellen einer Berichtsvorlage.

   - Wählen Sie den Unterordner **Verschlüsselte Geräte**, und starten Sie durch Klicken auf den Link **Bericht über Zugriffsrechte für verschlüsselte Geräte** den Assistenten für das Erstellen einer Berichtsvorlage.

3. Folgen Sie dem Assistenten für das Erstellen einer Berichtsvorlage.

Im Knoten **Administrationsserver** auf der Registerkarte **Berichte** wird ein neuer Bericht angezeigt. Der Vorgang zum Erstellen des Berichts wird gestartet. Der Bericht wird im Arbeitsplatz der Registerkarte **Berichte** angezeigt.

Um sich einen Bericht über Fehler bei der Verschlüsselung von Dateien und Ordnern anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Verschlüsselung und Datenschutz** aus.

2. Führen Sie eine der folgenden Aktionen aus:

   - Starten Sie durch Klicken auf den Link **Bericht über Fehler bei der Verschlüsselung von Dateien und Ordnern** im Verwaltungsblock **Fehler bei Datenverschlüsselung** den Assistenten für das Erstellen einer Berichtsvorlage.

   - Wählen Sie den Unterordner **Verschlüsselungsereignisse**, und starten Sie durch Klicken auf den Link **Bericht über Fehler bei der Verschlüsselung von Dateien und Ordnern** den Assistenten für das Erstellen einer Berichtsvorlage.

3. Folgen Sie dem Assistenten für das Erstellen einer Berichtsvorlage.

Im Knoten des Administrationsservers auf der Registerkarte **Berichte** wird der neue Bericht angezeigt. Der Vorgang zum Erstellen des Berichts wird gestartet. Der Bericht wird im Arbeitsplatz der Registerkarte **Berichte** angezeigt.

Um einen Bericht über den Verschlüsselungsstatus der Geräte anzeigen zu lassen, 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. Starten Sie über die Schaltfläche **Berichtsvorlage erstellen** den Assistenten für das Erstellen einer Berichtsvorlage.

4. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage auswählen** im Abschnitt **Sonstiges** den Punkt **Bericht über den Verschlüsselungsstatus der Geräte** aus.

   Nach Fertigstellen des Assistenten für das Erstellen einer Berichtsvorlage wird im Knoten Administrationsserver auf der Registerkarte **Berichte** die erstellte Berichtsvorlage angezeigt.

5. Wählen Sie im Knoten des benötigten Administrationsservers auf der Registerkarte **Berichte** die Vorlage für den Bericht, der in den vorherigen Schritten der Anleitung erstellt wurde.

Der Vorgang zum Erstellen des Berichts wird gestartet. Der Bericht wird im Arbeitsplatz der Registerkarte **Berichte** angezeigt.

Die Informationen darüber, inwieweit die Verschlüsselungsstatusvarianten von Geräten und Wechselmedien der Verschlüsselungsrichtlinie entsprechen, werden in den Informationsbereichen auf der Registerkarte **Statistik** im Knoten Administrationsserver angezeigt (s. Abschnitt "Statistik" auf S. 196).

Um sich einen Bericht über den gesperrten Zugriff auf Dateien anzeigen zu lassen, 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. Starten Sie über die Schaltfläche **Berichtsvorlage erstellen** den Assistenten für das Erstellen einer Berichtsvorlage.

4. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage auswählen** im Abschnitt **Sonstiges** den Punkt **Bericht über das Blockieren des Zugriffs auf Dateien** aus.

   Nach Fertigstellen des Assistenten für das Erstellen einer Berichtsvorlage wird im Knoten **Administrationsserver** auf der Registerkarte **Berichte** die erstellte Berichtsvorlage angezeigt.

5. Wählen Sie im Knoten **Administrationsserver** auf der Registerkarte **Berichte** die Vorlage für den Bericht, der in den vorherigen Schritten der Anleitung erstellt wurde.

Der Vorgang zum Erstellen des Berichts wird gestartet. Der Bericht wird im Arbeitsplatz der Registerkarte **Berichte** angezeigt.

Inventarisierung der im Netzwerk gefundenen Hardware

Kaspersky Security Center empfängt Informationen über die Hardware,
die bei einer Netzwerkabfrage gefunden wurde. Der Inventarisierung unterliegt jede ans Netzwerk angeschlossene Hardware. Bei jeder Netzwerkabfrage werden Informationen über
die Hardware aktualisiert. In der Liste der gefundenen Geräte können folgende Gerätetypen vorhanden sein:

- Geräte
- mobile Geräte
- Netzwerkgeräte
- virtuelle Geräte
- Computer-Hardware
- Computer-Peripheriegeräte
- angeschlossene Geräte
- VoIP-Telefonie
- Netzwerkspeicher.

Die bei einer Netzwerkabfrage gefundene Hardware wird im Unterordner **Datenverwaltung** des Ordners **Hardware** der Konsolenstruktur angezeigt.

Der Administrator kann neue Geräte zur Hardware-Liste manuell hinzufügen oder
die Informationen über die im Netzwerk bereits vorhandene Hardware bearbeiten.
In den Eigenschaften eines Geräts können Sie sich ausführliche Informationen über das Gerät anzeigen lassen und diese bearbeiten.

Der Administrator kann den gefundenen Geräten das Merkmal "Für Unternehmen" zuweisen.
Er kann dieses Merkmal in den Eigenschaften des Geräts manuell zuweisen oder die Kriterien

für die automatische Zuweisung festlegen. In diesem Fall wird das Merkmal "Für Unternehmen" nach dem Typ des Geräts zugewiesen. Nach dem Merkmal "Für Unternehmen" kann das Anschließen der Hardware zum Netzwerk zugelassen oder verboten werden.

Kaspersky Security Center ermöglicht es, eine Abschreibung von Hardware durchzuführen. Aktivieren Sie dazu in den Eigenschaften des Geräts das Kontrollkästchen **Das Gerät wurde abgeschrieben**. Ein solches Gerät wird in der Hardware-Liste nicht angezeigt.

In diesem Abschnitt

Informationen über neue Geräte hinzufügen

Um Informationen über neue Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Hardware**.
2. Öffnen Sie durch Klicken auf die Schaltfläche **Gerät hinzufügen** im Arbeitsplatz des Ordners **Hardware** das Fenster **Neues Gerät**.

   Das Fenster **Neues Gerät** wird geöffnet.
3. Wählen Sie im Fenster **Neues Gerät** in der Dropdown-Liste **Typ** den Typ des Gerätes aus, das Sie hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **OK**.

   Das Fenster mit den Geräte-Eigenschaften im Abschnitt **Allgemein** wird geöffnet.

5. Füllen Sie im Abschnitt **Allgemein** die Eingabefelder mit den Daten über das Gerät aus. Im Abschnitt **Allgemein** werden die folgenden Einstellungen angezeigt:

   - **Unternehmensgerät**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie dem Gerät das Merkmal "Für Unternehmen" zuweisen möchten. Nach diesem Merkmal können Sie Suche nach Geräten im Ordner **Hardware** durchführen.

   - **Das Gerät wurde abgeschrieben**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass das Gerät in der Geräteliste im Ordner **Hardware** angezeigt wird.

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Das neue Gerät wird im Arbeitsplatz des Ordners **Hardware** angezeigt.

Kriterien zur Bestimmung von Unternehmensgeräten anpassen

Um Kriterien zur Bestimmung von Unternehmensgeräten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Hardware**.

2. Öffnen Sie durch Klicken auf den Link **Kriterien zur Bestimmung von Unternehmensgeräten anpassen** im Arbeitsplatz des Ordners **Hardware** das Hardware-Eigenschaftenfenster.

3. Wählen Sie im Hardware-Eigenschaftenfenster im Abschnitt **Unternehmensgeräte** eine Methode für die Zuweisung dem Gerät des Merkmals "Für Unternehmen" aus:

   - **Das Merkmal "Für Unternehmen" für das Gerät manuell setzen**. Das Merkmal "Für Unternehmen" wird dem Gerät manuell im Eigenschaftenfenster des Geräts im Abschnitt **Allgemein** zugewiesen.

   - **Das Merkmal "Für Unternehmen" für das Gerät automatisch setzen**. Geben Sie in der Einstellungsgruppe **Nach dem Gerätetyp** die Gerätetypen an, denen das Programm das Merkmal "Für Unternehmen" automatisch zuweisen soll.

4. Klicken Sie auf die Schaltfläche **Übernehmen**.

Datenbanken-Update und Update der Programm-Module

In diesem Abschnitt werden der Download und die Verteilung von Updates für die Datenbanken und Programm-Module mithilfe von Kaspersky Security Center beschrieben.

Um den Schutz aufrechtzuerhalten, müssen Datenbanken und Programm-Module von Kaspersky Lab, die von Kaspersky Security Center verwaltet werden, stets rechtzeitig aktualisiert werden.

Die Aktualisierung der durch Kaspersky Security Center verwalteten Datenbanken und Programm-Module von Kaspersky Lab erfolgt über die Aufgabe **Herunterladen von Updates in die Datenverwaltung** des Administrationsservers. Nach der Ausführung der Aufgabe werden auf den Administrationsserver von der Update-Quelle Datenbanken und Updates der Programm-Module heruntergeladen werden.

> Die Aufgabe **Herunterladen von Updates in die Datenverwaltung** steht nicht auf virtuellen Administrationsservern zur Verfügung. In der Datenverwaltung des virtuellen Servers werden Updates angezeigt, die auf dem Haupt-Administrationsserver heruntergeladen wurden.

Sie können die Überprüfung von Updates auf Funktionstüchtigkeit und Fehlerfreiheit vor ihrer Installation auf den Client-Geräten anpassen.

Bei der Ausführung der Aufgabe **Herunterladen von Updates in den Speicher** werden zwecks Gewährleistung des Downloads erforderlicher Versionen von Datenbanken und Programmmodule an die Kaspersky Lab Update-Server folgende Informationen automatisch übermittelt:

- Identifikator und Version des Programms,
- Identifikator der Programminstallation;
- Identifikator des aktiven Schlüssels;
- Identifikator für den Start der Aufgabe **Herunterladen von Updates in die Datenverwaltung**.

Die übermittelten Informationen enthalten keine persönliche Daten und sonstige vertrauliche Daten. AO Kaspersky Lab schützt die erhaltenen Informationen in Übereinstimmung mit den geltenden gesetzlich festgelegten Anforderungen.

In diesem Abschnitt

Aufgabe Update-Download in den Speicher anlegen

Die Aufgabe für den Download von Updates in den Speicher des Administrationsservers wird automatisch bei der Ausführung des Schnellstartassistenten für Kaspersky Security Center erstellt. Die Aufgabe für den Download von Updates in den Speicher kann nur einmal erstellt werden. Deshalb können Sie eine Aufgabe für das Herunterladen von Updates in die Datenverwaltung nur dann erstellen, wenn sie aus der Liste mit Aufgaben des Administrationsservers entfernt wurde.

Um eine Aufgabe für das Herunterladen von Updates in die Datenverwaltung zu erstellen, gehen Sie wie folgt vor:

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

2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:

   - Wählen Sie im Kontextmenü des Ordners **Aufgaben** der Konsolenstruktur den Punkt **Erstellen** → **Aufgabe** aus.

   - Klicken Sie im Arbeitsplatz auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen. Im Fenster des Assistenten **Aufgabentyp** wählen Sie den Aufgabentyp **Herunterladen von Updates in die Datenverwaltung**.

Nach Ausführung des Assistenten erscheint die erstellte Aufgabe **Herunterladen von Updates in die Datenverwaltung** in der Liste mit Aufgaben des Administrationsservers.

Nach Fertigstellung der Aufgabe **Herunterladen von Updates in die Datenverwaltung** werden die Updates der Datenbanken und Programm-Module von der Update-Quelle geladen und im freigegebenen Ordner gespeichert. Wenn die Aufgabe für eine Administrationsgruppe erstellt wird, kommt sie nur auf Administrationsagenten zur Anwendung, die zur angegebenen Administrationsgruppe gehören.

Aus dem freigegebenen Ordner werden die Updates auf Client-Geräte und untergeordnete Administrationsserver verteilt.

Als Update-Quelle für den Administrationsserver können die folgenden Ressourcen verwendet werden:

- Kaspersky-Lab-Update-Server – Kaspersky-Lab-Server, auf denen sich die Updates der Datenbanken und Programm-Module befinden

- Hauptadministrationsserver

- FTP- / HTTP-Server oder Netzwerkordner für Updates – FTP- und HTTP-Server, lokaler Ordner oder Netzwerkordner, die vom Benutzer angegeben werden und Updates enthalten Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

Um den Administrationsserver von einem FTP- / HTTP-Server oder aus einem Netzwerkordner zu aktualisieren, kopieren Sie die richtige Ordnerstruktur mit den Updates auf diese Ressourcen, also die Struktur, die mit der bei Verwendung von Kaspersky-Lab-Update-Servern erstellten Struktur übereinstimmt.

Die Wahl der Ressource hängt von den Aufgabeneinstellungen ab. Standardmäßig erfolgt das Update aus dem Internet von den Kaspersky-Lab-Update-Servern.

Aufgabe für das Herunterladen von Updates in die Datenverwaltung der Update-Agenten erstellen

Um eine Aufgabe für den Download von Updates in den Speicher der Update-Agenten für eine ausgewählte Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wahlen Sie in der Konsolenstruktur den Ordner **Aufgaben** aus.
2. Starten Sie mithilfe der Schaltfläche **Aufgabe erstellen** im Arbeitsplatz des Ordners den Assistenten für die Erstellung von Aufgaben.
3. Wählen Sie im Fenster **Aufgabentyp** des Assistenten für die Erstellung von Aufgaben den Knoten **Kaspersky Security Center 10 Administrationsserver** aus, öffnen Sie den Ordner **Erweitert** und wählen Sie die Aufgabe **Erzwungenes Herunterladen von Updates in die Datenverwaltung der Update-Agenten** aus.
4. Folgen Sie den Schritten des Assistenten.

Nach Fertigstellung des Assistenten erscheint die erstellte Aufgabe **Erzwungenes Herunterladen von Updates in die Datenverwaltung der Update-Agenten** in der Aufgabenliste des Administrationsagenten in der entsprechenden Administrationsgruppe und im Ordner **Aufgaben**.

Bei der Ausführung der Aufgabe **Erzwungenes Herunterladen von Updates in die Datenverwaltung der Update-Agenten** werden die Updates der Datenbanken und Programm-Module aus der Update-Quelle heruntergeladen und im freigegebenen Ordner gespeichert. Die Ergebnisse der Aufgabenausführung werden nur von jenen Update-

Agenten der angegebenen Administrationsgruppe verwendet, denen die Aufgabe des Administrationsservers **Herunterladen von Updates in die Datenverwaltung** nicht zugewiesen wurde.

Wenn die Aufgabe **Erzwungenes Herunterladen von Updates in die Datenverwaltung der Update-Agenten** für eine Gruppe von Geräten erstellt wird, ist der Netzwerkordner für Updates für den Administrator nicht verfügbar.

Wenn eine lokale Aufgabe **Erzwungenes Herunterladen von Updates in die Datenverwaltung der Update-Agenten** für ein Gerät erstellt wird, ist der Netzwerkordner für Updates für den Administrator verfügbar.

Konfiguration der Aufgabe für das Herunterladen von Updates in die Datenverwaltung

Um die Einstellungen der Aufgabe für das Herunterladen von Updates in die Datenverwaltung anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz des Ordners **Aufgaben** der Konsolenstruktur die Aufgabe **Herunterladen von Updates in die Datenverwaltung** in der Aufgabenliste aus.

2. Öffnen Sie das Eigenschaftenfenster der Aufgabe auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Eigenschaften** aus.

   - Klicken Sie im Arbeitsplatz der gewählten Aufgabe auf den Link **Aufgabeneinstellungen ändern**.

   Daraufhin wird das Eigenschaftenfenster der Aufgabe **Herunterladen von Updates in die Datenverwaltung** geöffnet. Hier können Sie die Einstellungen für das Herunterladen von Updates in die Datenverwaltung des Administrationsservers anpassen.

Heruntergeladene Updates überprüfen

Damit Kaspersky Security Center die empfangenen Updates überprüft, bevor sie auf die Client-Geräte verteilt werden, gehen Sie wie folgt vor:

1. Wählen Sie im Arbeitsplatz des Ordners **Aufgaben** der Konsolenstruktur in der Aufgabenliste die Aufgabe **Herunterladen von Updates in die Datenverwaltung** aus.

2. Öffnen Sie das Eigenschaftenfenster der Aufgabe auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie im Arbeitsplatz der gewählten Aufgabe auf den Link **Aufgabeneinstellungen ändern**.

3. Aktivieren Sie im folgenden Eigenschaftenfenster der Aufgabe im Abschnitt **Update-Prüfung** das Kontrollkästchen **Update-Prüfung vor der Verteilung ausführen**, und wählen Sie die Aufgabe zur Update-Prüfung auf eine der folgenden Weisen aus:

   - Klicken Sie auf **Auswählen**, um die erstellte Aufgabe zur Update-Prüfung auszuwählen.

   - Klicken Sie auf **Erstellen**, um die Aufgabe zur Update-Prüfung zu erstellen.

     Daraufhin wird der Assistent für die Erstellung von Aufgaben zur Update-Überprüfung gestartet. Folgen Sie den Anweisungen.

     Beim Erstellen einer Aufgabe zur Update-Überprüfung müssen Sie die Administrationsgruppe auswählen, auf deren Geräten diese Aufgabe ausgeführt werden soll. Die zu dieser Gruppe gehörenden Geräte werden als *Testgeräte* bezeichnet.

     > Es wird empfohlen, gut geschützte Geräte mit einer Programmkonfiguration, die im Unternehmensnetzwerk am weitesten verbreitet ist, als Testgeräte zu verwenden. Dadurch wird die Qualität der Überprüfung erhöht und das Risiko von Fehlalarmen und Virenfunden verringert (wenn Viren auf den Testgeräten gefunden werden, gilt die Aufgabe zur Update-Prüfung als nicht erfolgreich abgeschlossen).

4. Schließen Sie das Eigenschaftenfenster der Aufgabe für das Herunterladen von Updates in die Datenverwaltung, indem Sie auf **OK** klicken.

Daraufhin wird im Rahmen der Aufgabe für das Herunterladen von Updates in die Datenverwaltung die Aufgabe zur Prüfung der empfangenen Updates ausgeführt. Der Administrationsserver kopiert Updates aus der Quelle, speichert sie in einem temporären Verzeichnis und startet die Aufgabe zur Update-Prüfung. Wird diese Aufgabe erfolgreich abgeschlossen, werden die Updates aus der temporären Datenverwaltung in den freigegebenen Ordner des Administrationsservers kopiert (<Kaspersky Security Center Installationsverzeichnis>\Share\Updates) und auf Client-Geräte verteilt, für die der Administrationsserver die Update-Quelle ist.

Wenn in den Ergebnissen der Aufgabe zur Update-Prüfung die im temporären Verzeichnis liegenden Updates als fehlerhaft eingestuft werden oder wenn die Aufgabe mit einem Fehler beendet wird, werden die Updates nicht im freigegebenen Ordner gespeichert.
Auf dem Administrationsserver verbleibt das vorherige Update. Die Aufgaben der Zeitplanart **Nach dem Herunterladen von Updates in die Datenverwaltung** werden ebenfalls nicht gestartet. Diese Vorgänge werden beim nächsten Ausführen der Aufgabe für das Herunterladen von Updates in die Datenverwaltung gestartet, wenn die Prüfung der neuen Updates erfolgreich verläuft.

Das Update gilt als fehlerhaft, wenn mindestens ein Testgerät eine der folgenden Bedingungen erfüllt:

- Es ist ein Fehler in einer Update-Aufgabe aufgetreten.
- Nach Übernahme der Updates hat sich der Status des Echtzeitschutzes des Schutzprogramms geändert.
- Im Verlauf der Aufgabe zur Untersuchung auf Anforderung wurde ein infiziertes Objekt gefunden.
- Es ist ein Funktionsfehler im Kaspersky-Lab-Programm aufgetreten.

Wenn auf keinem Testgerät eine der genannten Bedingungen erfüllt wurde, wird das Set an Updates als ordnungsgemäß anerkannt und die Aufgabe zur Update-Prüfung gilt als erfolgreich abgeschlossen.

Konfiguration der Prüfungsrichtlinien und Hilfsaufgaben

Beim Erstellen einer Aufgabe zur Update-Prüfung legt der Administrationsserver Prüfungsrichtlinien sowie Hilfsgruppenaufgaben zum Update und zur Untersuchung auf Befehl an.

> Die Durchführung von Hilfsgruppenaufgaben zum Update und zur Virensuche auf Befehl kann einige Zeit in Anspruch nehmen. Diese Aufgaben werden im Rahmen der Aufgabe zur Update-Prüfung durchgeführt. Die Aufgabe zur Update-Prüfung wird im Rahmen der Aufgabe für den Download von Updates in den Speicher durchgeführt. Die Zeit, die für die Aufgabe für das Herunterladen von Updates in die Datenverwaltung benötigt wird, umfasst auch die Zeit für Hilfsgruppenaufgaben zum Update und zur Virensuche auf Befehl.

Die Einstellungen für die Prüfungsrichtlinien und Hilfsaufgaben können geändert werden.

Um die Einstellungen der Prüfungsrichtlinie oder einer Hilfsaufgabe zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum die Gruppe, für die die Aufgabe zur Update-Prüfung erstellt wurde.

2. Klicken Sie im Arbeitsplatz auf eine der folgenden Registerkarten:

   - **Richtlinien**, wenn Sie die Einstellungen der Prüfungsrichtlinie ändern möchten

   - **Aufgaben**, wenn Sie die Einstellungen der Hilfsaufgabe ändern möchten.

3. Wählen Sie im Arbeitsplatz der Registerkarte die Richtlinie oder die Aufgabe, deren Einstellungen Sie ändern möchten.

4. Öffnen Sie das Eigenschaftenfenster dieser Richtlinie (Aufgabe) auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Richtlinie (Aufgabe), und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf **Richtlinieneinstellungen ändern** (**Aufgabeneinstellungen ändern**) im Arbeitsbereich der ausgewählten Richtlinie (Aufgabe).

Damit die Update-Prüfung korrekt erfolgen kann, müssen die Änderungen der Einstellungen der Prüfungsrichtlinien und Hilfsaufgaben unter folgenden Aspekten vorgenommen werden:

- In den Einstellungen für Hilfsaufgaben:
  - Es müssen alle Ereignisse der Ereigniskategorie **Kritisches Ereignis** und **Funktionsfehler** auf dem Administrationsserver gespeichert werden.
    Der Administrationsserver analysiert den Programmverlauf aufgrund von Ereignissen dieser Arten.
  - Als Update-Quelle muss der Administrationsserver verwendet werden.
  - Die Zeitplanart für die Aufgaben muss angegeben werden: **Manuell**.
- In den Einstellungen der Prüfungsrichtlinien:
  - Die Beschleunigungstechnologien iChecker, iSwift und iStream dürfen nicht verwendet werden.
  - Es muss eine Aktion für infizierte Objekte ausgewählt werden: **Nicht erfragen** / **Überspringen** / **Protokollieren**.
- In den Einstellungen der Prüfungsrichtlinien und Hilfsaufgaben:

  Wenn nach der Installation der Updates für die Programm-Module ein Neustart des Geräts erforderlich ist, muss dieser unverzüglich ausgeführt werden. Wenn das Gerät nicht neu gestartet wird, kann die Richtigkeit dieses Typs von Updates nicht überprüft werden.
  Bei einigen Anwendungen kann die Installation der Updates, die einen Neustart erfordern, unterdrückt sein oder erst nach Bestätigung durch den Benutzer erfolgen.
  Diese Beschränkungen müssen in den Einstellungen der Prüfungsrichtlinien und Hilfsaufgaben deaktiviert sein.

Heruntergeladene Updates anzeigen

Um die Liste der heruntergeladenen Updates anzusehen,

wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Updates und Patches für Software von Kaspersky Lab**.

Im Arbeitsplatz des Ordners **Updates und Patches für Software von Kaspersky Lab** wird eine Liste der Updates angezeigt, die im Speicher des Administrationsservers gespeichert sind.

Updates automatisch verteilen

Kaspersky Security Center ermöglicht es, Updates automatisch auf Client-Geräte und untergeordnete Administrationsserver zu verteilen und darauf zu installieren.

In diesem Abschnitt

Updates automatisch auf Client-Geräte verteilen

Damit Updates für das ausgewählte Programm direkt nach dem Update-Download in die Datenverwaltung des Administrationsservers automatisch auf die Client-Geräte verteilt werden, gehen Sie wie folgt vor:

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

2. Erstellen Sie eine Aufgabe zur Verteilung der Updates dieses Programms für ausgewählte Client-Geräte auf eine der folgenden Weisen:

   - Wenn es erforderlich ist, Updates auf die zur gewählten Administrationsgruppe gehörenden Client-Geräte zu verteilen, erstellen Sie eine Aufgabe für die gewählte Gruppe (s. Abschnitt "Gruppenaufgaben erstellen" auf S. 136).

   - Wenn es erforderlich ist, Updates auf die Client-Geräte zu verteilen, die zu unterschiedlichen Administrationsgruppen gehören, erstellen Sie eine Aufgabe für bestimmte Geräte (s. Abschnitt "Aufgabe für bestimmte Geräte erstellen" auf S. 138).

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie seinen Anweisungen, indem Sie wie folgt vorgehen:

   a. Im Fenster des Assistenten **Aufgabentyp** im Knoten des entsprechenden Programms wählen Sie die Aufgabe zur Verteilung der Updates.

   > Die Bezeichnung der Aufgabe zur Verteilung von Updates, die im Fenster **Aufgabentyp** angezeigt wird, hängt vom Programm ab, für welches die Aufgabe erstellt wird. Für ausführliche Informationen über die Bezeichnungen der Update-Aufgaben für ausgewählte Programme von Kaspersky Lab, siehe Handbücher zu diesen Programmen.

   b. Im Fenster des Assistenten **Zeitplan** im Feld **Start nach Zeitplan** wählen Sie die Startvariante **Nach dem Herunterladen von Updates in die Datenverwaltung**.

   Die Aufgabe zur Verteilung von Updates wird für ausgewählte Geräte jedes Mal nach dem Herunterladen von Updates in die Datenverwaltung des Administrationsservers gestartet.

Wenn die Aufgabe zur Verteilung von Updates eines bestimmten Programms für ausgewählte Geräte bereits erstellt wurde, muss für die automatische Verteilung der Updates auf Client-Geräte im Eigenschaftenfenster im Abschnitt **Zeitplan** die Startvariante **Nach dem Herunterladen von Updates in die Datenverwaltung** im Feld **Start nach Zeitplan** ausgewählt werden.

Updates automatisch auf untergeordnete Administrationsserver verteilen

Damit Updates für das ausgewählte Programm direkt nach dem Update-Download in die Datenverwaltung des Hauptadministrationsservers automatisch auf untergeordnete Administrationsserver verteilt werden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Knoten des Hauptadministrationsservers den Ordner **Aufgaben** aus.

2. In der Aufgabenliste des Arbeitsplatzes wählen Sie die Aufgabe für das Herunterladen von Updates in die Datenverwaltung des Administrationsservers.

3. Öffnen Sie den Abschnitt **Einstellungen** im Eigenschaftenfenster der ausgewählten Aufgabe auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie im Arbeitsplatz der gewählten Aufgabe auf den Link **Einstellungen anpassen**.

4. Öffnen Sie im Abschnitt **Einstellungen** im Eigenschaftenfenster der Aufgabe das Fenster **Sonstige Einstellungen**, indem Sie auf den Link **Anpassen** im Unterabschnitt **Sonstige Einstellungen** klicken.

5. Im folgenden Fenster **Sonstige Einstellungen** aktivieren Sie das Kontrollkästchen **Update untergeordneter Server erzwingen**.

Aktivieren Sie im Eigenschaftenfenster der Aufgabe Update-Download durch Administrationsserver auf der Registerkarte **Einstellungen** das Kontrollkästchen **Update untergeordneter Server erzwingen**.

Nach Abschluss des Update-Downloads durch den Hauptadministrationsserver werden jetzt automatisch die Aufgaben des Update-Downloads durch untergeordnete Administrationsserver gestartet, und zwar unabhängig von dem Zeitplan, der in den Aufgabeneinstellungen angegeben ist.

Automatische Installation der Programm-Module der Administrationsagenten

Damit die Updates der Programm-Module der Administrationsagenten nach ihrem Download in die Datenverwaltung des Administrationsservers automatisch installiert werden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Knoten des Hauptadministrationsservers den Ordner **Aufgaben** aus.
2. In der Aufgabenliste im Arbeitsplatz wählen Sie eine Aufgabe für das Herunterladen von Updates in die Datenverwaltung des Administrationsservers aus.
3. Öffnen Sie das Eigenschaftenfenster der gewählten Aufgabe auf eine der folgenden Weisen:
   - Klicken Sie mit der rechten Maustaste auf die Aufgabe, und wählen Sie **Eigenschaften** aus.
   - Klicken Sie im Arbeitsplatz der gewählten Aufgabe auf den Link **Einstellungen anpassen**.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
5. Öffnen Sie über den Link **Anpassen** im Block **Sonstige Einstellungen** das Fenster **Sonstige Einstellungen**.
6. Im folgenden Fenster **Sonstige Einstellungen** aktivieren Sie das Kontrollkästchen **Module der Administrationsagenten updaten**.

   Wenn das Kontrollkästchen aktiviert ist, werden die Updates der Programm-Module der Administrationsagenten nach ihrem Download automatisch in die Datenverwaltung des Administrationsservers installiert. Ist das Kontrollkästchen deaktiviert, wird die automatische Installation von Updates des Administrationsagenten nicht ausgeführt. Die erhaltenen Updates können manuell installiert werden. Dieses Kontrollkästchen ist standardmäßig aktiviert.

   > Die automatische Installation der Programm-Module der Administrationsagenten ist nur für die Administrationsagenten der Version 10 Service Pack 1 und niedriger verfügbar.

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

Anschließend werden die Updates der Programm-Module der Administrationsagenten automatisch installiert.

Geräte zum Update-Agenten bestimmen

In Kaspersky Security Center haben Sie die Möglichkeit, Geräte zu Update-Agenten zu bestimmen. Dies kann automatisch (mithilfe des Administrationsservers) oder manuell durchgeführt werden.

Wenn in der Struktur der Administrationsgruppen die Netzwerktopologie abgebildet wird oder bestimmte Teile des Netzwerks einer bestimmten Administrationsgruppe entsprechen, kann die automatische Festlegung von Update-Agenten verwendet werden.

Wenn der Strukturaufbau der Administrationsgruppen nicht die Netzwerktopologie widerspiegelt, wird empfohlen, die automatische Bestimmung von Update-Agenten zu deaktivieren und in den jeweiligen Teilen des Netzwerks einen oder mehrere Geräte manuell zu Update-Agenten zu bestimmen.

> Es wird empfohlen, bei der manuellen Festlegung von Update-Agenten einen Update-Agenten für jeweils 100–200 bearbeitete Geräte zu bestimmen.

Um ein Gerät manuell zum Update-Agenten zu bestimmen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **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 aus, das die Rolle des Update-Agenten übernehmen soll (wählen Sie dieses in der Administrationsgruppe aus oder geben Sie die IP-Adresse des Geräts an). 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 (s. Abschnitt "Update-Agent" auf S. 90).

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.

6. Wählen Sie den hinzugefügten Update-Agent in der Liste aus und öffnen Sie mithilfe der Schaltfläche **Eigenschaften** das entsprechende Eigenschaftenfenster.

7. Passen Sie im Eigenschaftenfenster die Einstellungen des Update-Agenten an:

   - Geben Sie im Abschnitt **Allgemein** die Nummer des SSL-Ports, Adresse und Port des IP-Multicast sowie das Datenkontingent an, das vom Update-Agent verteilt werden soll (der Update-Agent kann Updates und/oder Installationspakete verteilen).
   - Geben Sie im Abschnitt **Gültigkeitsbereich** den Bereich an, auf den der Update-Agent die Updates verteilen soll (Administrationsgruppen und/oder NLA-Subnet).
   - Passen Sie im Abschnitt **Netzwerkabfrage** die Einstellungen für die Abfrage der Windows-Domänen, des Active Directory oder des IP-Bereichs durch den Update-Agenten an.
   - Geben Sie im Abschnitt **Erweitert** den Ordner an, den der Update-Agent zum Speichern der zu verteilenden Daten verwenden soll.

Daraufhin übernehmen die ausgewählten Geräte die Rolle des Update-Agenten.

Um die Update-Agenten automatisch mithilfe des Administrationsservers festzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Aktivieren Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Update-Agenten** das Kontrollkästchen **Update-Agenten automatisch bestimmen**.

   > Wenn die automatische Bestimmung der Update-Agenten aktiviert ist, dürfen die Einstellungen der Update-Agenten nicht manuell angepasst werden und die Liste der Update-Agenten darf nicht verändert werden.

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

Daraufhin beginnt der Administrationsserver damit, Update-Agenten automatisch zu bestimmen und ihre Einstellungen zu konfigurieren.

Gerät aus der Liste der Update-Agenten entfernen

Um ein Gerät aus der Liste der Update-Agenten zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Update-Agenten** ein Gerät aus, das als Update-Agent dient, und klicken Sie auf die Schaltfläche **Entfernen**.

Daraufhin wird das Gerät aus der Liste der Update-Agenten entfernt und übernimmt nicht länger die Funktion eines Update-Agenten.

> Ein Gerät, dem automatisch die Rolle des Administrationsservers zugewiesen wurde, kann nicht aus der Liste der Update-Agenten gelöscht werden (s. Abschnitt "Geräte zum Update-Agenten bestimmen" auf S. 346).

Updates über Update-Agenten empfangen

In Kaspersky Security Center können die Update-Agenten Updates vom Administrationsserver, von den Servern von Kaspersky Lab, aus lokalen oder Netzwerkordnern abrufen.

Um den Update-Download für den Update-Agenten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver**.
2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.
3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Update-Agenten** den Update-Agenten aus, über den Updates auf die Client-Geräte der Gruppe heruntergeladen werden sollen.
4. Öffnen Sie mithilfe der Schaltfläche **Eigenschaften** das Eigenschaftenfenster des Update-Agenten.
5. Wählen Sie im Eigenschaftenfenster des Agenten den Abschnitt **Update-Quelle**.
6. Wählen Sie die Update-Quelle für den Update-Agenten:
   - Damit der Update-Agent die Updates vom Administrationsserver erhält, wählen Sie die Option **Vom Administrationsserver beziehen**.
   - Damit der Update-Agent die Updates mithilfe von Aufgaben erhält, wählen Sie die Option **Aufgabe Update-Download verwenden**.
     - Klicken Sie auf **Auswählen**, um die erstellte Aufgabe Update-Download durch den Update-Agenten auszuwählen.
     - Klicken Sie auf die Schaltfläche **Neue Aufgabe**, um eine Aufgabe Update-Download durch den Update-Agenten zu erstellen.

     > Die Aufgabe zum Update-Download durch den Update-Agent ist eine lokale Aufgabe. Für jedes Gerät, das die Rolle eines Update-Agenten übernimmt, muss eine separate Aufgabe zum Update-Download erstellt werden.

Daraufhin bezieht der Update-Agent die Updates von der angegebenen Quelle.

Installierte Updates zurücksetzen

Gehen Sie folgendermaßen vor, um installierte Updates zurückzusetzen:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Software-Updates** aus.

2. Wählen Sie im Arbeitsplatz des Ordners **Software-Updates** das Update, das zurückgesetzt werden soll.

3. Wählen Sie im Kontextmenü des Updates die Option **Update-Dateien löschen**.

4. Starten Sie die Update-Aufgabe (s. Abschnitt "Updates für Kaspersky Endpoint Security automatisch auf den Geräten installieren" auf S. 242).

Nach der Ausführung der Aufgabe wird das auf dem Client-Gerät installierte Update zurückgesetzt und erhält den Status **Nicht installiert**.

Arbeit mit den Schlüsseln für Programme

In diesem Abschnitt werden die Möglichkeiten von Kaspersky Security Center bei der Arbeit mit Schlüsseln von Programmen beschrieben, die von Kaspersky Lab verwaltet werden.

Kaspersky Security Center ermöglicht eine zentrale Verteilung von Schlüsseln für Kaspersky-Lab-Programme auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung der Gültigkeitsdauer der Lizenz.

Beim Hinzufügen eines Schlüssels über Kaspersky Security Center werden die Schlüssel-Einstellungen auf dem Administrationsserver gespeichert. Anhand dieser Informationen erstellt das Programm einen Bericht über die Schlüsselnutzung und informiert den Administrator über den Ablauf der Gültigkeitsdauer von Lizenzen und eine Überschreitung der in den Schlüssel-Einstellungen vorgegebenen Lizenzbeschränkungen. Sie können die Einstellungen für Benachrichtigungen über die Schlüsselverwendung in den Einstellungen des Administrationsservers konfigurieren.

In diesem Abschnitt

Informationen zu verwendeten Schlüsseln anzeigen

Um sich Informationen über die verwendeten Schlüssel anzeigen zu lassen,

wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzen für Kaspersky-Lab-Software** aus.

Im Arbeitsplatz des Ordners wird eine Liste der Schlüssel angezeigt, die auf den Client-Geräten verwendet werden.

Neben jedem Schlüssel wird ein Symbol angezeigt, das dem Typ der Schlüsselverwendung entspricht:

-  – Daten über den verwendeten Schlüssel, die von dem mit dem Administrationsserver verbundenen Client-Gerät empfangen wurden. Die Schlüsseldatei wird auf dem Administrationsserver nicht gespeichert.
-  – Die Schlüsseldatei befindet sich im Speicher des Administrationsservers. Die automatische Verteilung des Schlüssels wurde deaktiviert.
-  – Die Schlüsseldatei befindet sich im Speicher des Administrationsservers. Die automatische Verteilung des Schlüssels wurde aktiviert.

Sie können im Eigenschaftenfenster des Client-Geräts im Abschnitt **Programme** Informationen darüber anzeigen lassen, welche Schlüssel für ein Programm auf einem Client-Gerät verwendet werden (s. Abschnitt "Lokale Programmeinstellungen anzeigen und ändern" auf S. 148).

Zur Bestimmung der aktuellen Einstellungen für die Schlüssel des virtuellen Administrationsservers sendet der Administrationsserver mindestens einmal pro Stunde eine Anfrage an die Aktivierungsserver von Kaspersky Lab.

Schlüssel zum Speicher des Administrationsservers hinzufügen

Um einen Schlüssel zur Datenverwaltung des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzen für Kaspersky-Lab-Software** aus.

2. Starten Sie die Aufgabe für das Hinzufügen von Schlüsseln auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Liste der Schlüssel und wählen Sie **Schlüssel hinzufügen** aus.

   - Klicken Sie im Verwaltungsblock mit der Liste der Schlüssel auf den Link **Schlüssel hinzufügen**.

   Daraufhin wird der Assistent zum Hinzufügen von Schlüsseln gestartet. Folgen Sie den Anweisungen.

Schlüssel des Administrationsservers löschen

Um einen Schlüssel für den Administrationsserver zu löschen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

2. Wählen Sie im folgenden Eigenschaftenfenster des Administrationsservers den Abschnitt **Schlüssel** aus.

3. Löschen Sie den aktiven bzw. Reserveschlüssel mithilfe der Schaltfläche **Löschen**.

   Der Schlüssel wird daraufhin gelöscht.

Wenn ein Reserveschlüssel hinzugefügt worden ist, wird nach dem Löschen des aktiven Schlüssels der Reserveschlüssel automatisch zum aktiven Schlüssel.

Nach dem Löschen des aktiven Schlüssels sind die Funktionen **Systems Management** (s. Abschnitt "**Lizenzierungsvarianten für Kaspersky Security Center**" auf S. 67) und **Mobile Geräte verwalten** (s. Abschnitt "**Lizenzierungsvarianten für Kaspersky Security Center**" auf S. 67) auf dem Administrationsserver nicht verfügbar. Ein gelöschter Schlüssel kann erneut hinzugefügt (s. Abschnitt "Schlüssel zum Speicher des Administrationsservers hinzufügen" auf S. 353) oder durch einen anderen Schlüssel ersetzt werden.

Schlüssel auf Client-Geräte verteilen

Kaspersky Security Center ermöglicht die Verteilung von Schlüsseln auf Client-Geräte mit der Aufgabe zur Schlüsselverteilung.

Um einen Schlüssel auf Client-Geräte zu verteilen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzen für Kaspersky-Lab-Software** aus.

2. Klicken Sie im Verwaltungsblock mit der Liste der Schlüssel auf die Schaltfläche **Schlüssel auf verwaltete Geräte verteilen**.

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

Aufgaben, die mit dem Assistenten für das Erstellen einer Aufgabe zur Schlüsselverteilung erstellt wurden, gelten als Aufgaben für bestimmte Geräte und werden im Ordner **Aufgaben** der Konsolenstruktur abgelegt.

Außerdem können Sie eine Gruppenaufgabe oder eine lokale Aufgabe zur Schlüsselverteilung mithilfe des Assistenten für das Erstellen einer Aufgabe für eine Administrationsgruppe und für ein Client-Gerät erstellen.

Schlüssel automatisch verteilen

Kaspersky Security Center ermöglicht das automatische Verteilen von Schlüsseln, die sich im Schlüsselspeicher auf dem Administrationsserver befinden, auf die verwalteten Geräte.

Um einen Schlüssel automatisch auf die verwalteten Geräte zu verteilen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Programmverwaltung** den Unterordner **Lizenzen für Kaspersky-Lab-Software** aus.

2. Wählen Sie im Arbeitsplatz des Ordners den Schlüssel, den Sie automatisch auf die Geräte verteilen möchten.

3. Öffnen Sie das Eigenschaftenfenster des gewählten Schlüssels auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf den Schlüssel und wählen Sie **Eigenschaften** aus.

   - Klicken Sie im Block des gewählten Schlüssels auf den Link **Schlüssel-Einstellungen anzeigen**.

4. Aktivieren Sie im folgenden Eigenschaftenfenster des Schlüssels **Automatisch zu verteilender Schlüssel**. Schließen Sie das Eigenschaftenfenster des Schlüssels.

Daraufhin wird der Schlüssel automatisch als aktiver Schlüssel oder Reserveschlüssel auf die passenden Geräte verteil.

Die Verteilung des Schlüssels erfolgt durch den Administrationsagenten. Es werden dabei keine Hilfsaufgaben zur Verteilung eines Schlüssels für ein Programm angelegt.

Bei der automatischen Verteilung des Schlüssels als aktiver Schlüssel oder Reserveschlüssel werden die Lizenzbeschränkungen hinsichtlich der in den Schlüssel-Einstellungen festgelegten Anzahl der Geräte berücksichtigt. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Schlüssels auf Geräte automatisch beendet.

Bericht über die Schlüsselverwendung erstellen und anzeigen

Um einen Bericht über die Schlüsselnutzung auf Client-Geräten zu erstellen, 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 die Vorlage des Berichts **Bericht über die Schlüsselnutzung** oder erstellen Sie eine neue Vorlage für den Bericht des gleichnamigen Typs.

Daraufhin werden im Arbeitsplatz des Berichts über die Schlüsselnutzung Informationen über aktive Schlüssel und Reserve-Schlüssel angezeigt, die auf den Client-Geräten verwendet werden. Darüber hinaus enthält der Bericht Informationen über Geräte, auf denen Schlüssel verwendet werden, und über die in den Schlüsseleinstellungen vorgegebenen Einschränkungen.

Datenverwaltung

Dieser Abschnitt enthält Informationen zu Daten, die auf dem Administrationsserver gespeichert und zur Überwachung und Wartung von Client-Geräten verwendet werden.

Daten, die zur Statusverfolgung der Geräte und deren Wartung verwendet werden, werden in der Konsolenstruktur im Ordner **Datenverwaltung** angezeigt.

Der Ordner **Datenverwaltung** enthält die folgenden Objekte:

- durch den Administrationsserver heruntergeladene Updates, die auf Client-Geräte verteilt werden (s. Abschnitt "Heruntergeladene Updates anzeigen" auf S. 341);
- Liste der im Netzwerk gefundenen Hardware;
- auf den Client-Geräten gefundene Schlüssel (s. Abschnitt "Arbeit mit den Schlüsseln für Programme" auf S. 351);
- Dateien, die von Schutzprogrammen in den Quarantäneordnern auf den Geräten gespeichert wurden;
- Dateien, die auf Client-Geräten in Backups verschoben wurden;
- Dateien, für die Schutzprogramme eine verschobene Untersuchung festgelegt haben.

In diesem Abschnitt

Liste mit Objekten, die sich in der Datenverwaltung befinden, in eine Textdatei exportieren

Sie können alle Objekte, die sich der Datenverwaltung befinden, in eine Textdatei exportieren.

Um die Objektliste der Datenverwaltung in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum aus dem Ordner **Datenverwaltung** den Unterordner der gewünschten Datenverwaltung.

2. Klicken Sie mit der rechten Maustaste auf die Objektliste der Datenverwaltung und wählen Sie **Liste exportieren**.

   Daraufhin öffnet sich das Fenster **Liste exportieren**, in dem Sie den Namen der Textdatei und den Ordnerpfad angeben können.

Installationspakete

Kaspersky Security Center legt Installationspakete für Kaspersky-Lab-Programme und Programme von Drittherstellern in der Datenverwaltung ab.

Das *Installationspaket* besteht aus mehreren Dateien, die für die Installation des Programms erforderlich sind. Das Installationspaket enthält Einstellungen zum Installationsvorgang und zur Erstkonfiguration des Programms.

Wenn Sie ein Programm auf einem Client-Gerät installieren möchten, müssen Sie für dieses Programm ein Installationspaket erstellen (s. Abschnitt "Installationspakete für Programme erstellen" auf S. 264) oder ein bereits erstelltes Installationspaket verwenden. Die Liste aller erstellten Installationspakete befindet sich im Konsolenbaum im Ordner **Remote-Installation** im Unterordner **Installationspakete**.

Nähere Informationen zu Installationspaketen finden Sie im *Implementierungshandbuch von Kaspersky Security Center*.

Quarantäne und Backup

Auf den Client-Geräten installierte Antiviren-Programme von Kaspersky Lab können während der Untersuchung von Geräten Dateien in Quarantäne oder ins Backup verschieben.

Die *Quarantäne* ist ein spezieller Speicher, in den Dateien verschoben werden, die möglicherweise von Viren infiziert oder im Augenblick des Funds irreparabel sind.

Das *Backup* dient zur Speicherung der Sicherungskopien von Dateien, die gelöscht oder bei der Desinfizierung verändert wurden.

Kaspersky Security Center erstellt eine gemeinsame Liste von Dateien, die von Kaspersky-Lab-Programmen auf den Client-Geräten in die Quarantäne oder ins Backup verschoben werden. Die Administrationsagenten der Client-Geräte leiten Informationen über die Dateien in der Quarantäne und im Backup an den Administrationsserver weiter.
Über die Verwaltungskonsole können Sie die Eigenschaften der Dateien in der Datenverwaltung der Geräte ansehen, die Untersuchung der Datenverwaltung auf Viren starten und Dateien aus der Datenverwaltung löschen.

> Quarantäne und Backup sind für Kaspersky Anti-Virus für Windows Workstation und Kaspersky Anti-Virus für Windows Server Version 6.0 und höher sowie für Kaspersky Endpoint Security 10 für Windows verfügbar.

Kaspersky Security Center kopiert keine Dateien aus der Datenverwaltung auf den Administrationsserver. Alle Dateien werden in der Datenverwaltung auf den Geräten abgelegt. Die Wiederherstellung der Dateien wird auf dem Gerät mit dem installierten Schutzprogramm ausgeführt, das die Datei in die Datenverwaltung verschoben hat.

In diesem Abschnitt

Aktivieren der Remote-Verwaltung von Dateien in der Datenverwaltung

Standardmäßig ist die Remote-Verwaltung von Dateien in der Datenverwaltung auf den Client-Geräten deaktiviert.

Um die Remote-Verwaltung von Dateien in der Datenverwaltung auf den Client-Geräten zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum die Administrationsgruppe, für die die Remote-Verwaltung der Dateien aktiviert werden soll.
2. Öffnen Sie im Arbeitsplatz der Gruppe die Registerkarte **Richtlinien**.
3. Wählen Sie unter **Richtlinien** die Richtlinie des Schutzprogramms, welche die Dateien auf den Geräten in die Datenverwaltung verschiebt.
4. Aktivieren Sie im Fenster der Richtlinieneigenschaften unter **Administrationsserver benachrichtigen** die Kontrollkästchen jeder Datenverwaltungsart, für die Sie die Remote-Verwaltung aktivieren möchten.

Die Lage des Blocks **Administrationsserver benachrichtigen** im Fenster der Richtlinieneigenschaften sowie die Beschriftungen der Kontrollkästchen sind spezifisch für jedes Schutzprogramm.

Eigenschaften der Datei in der Datenverwaltung anzeigen

Um Eigenschaften einer Datei in Quarantäne oder im Backup anzusehen, gehen Sie wie folgt vor:

1. In der Konsolenstruktur im Ordner **Datenverwaltung** öffnen Sie den Unterordner **Quarantäne** oder **Backup**.

2. Im Arbeitsplatz des Ordners **Quarantäne** (**Backup**) wählen Sie die Datei aus, deren Eigenschaften angezeigt werden sollen.

3. Öffnen Sie das Eigenschaftenfenster der Datei auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Eigenschaften** aus.

   - Klicken Sie auf den Link **Objekteigenschaften öffnen** im Bearbeitungsblock der ausgewählten Datei.

Dateien aus der Datenverwaltung entfernen

Um eine Datei in Quarantäne oder im Backup zu löschen, gehen Sie wie folgt vor:

1. In der Konsolenstruktur im Ordner **Datenverwaltung** öffnen Sie den Unterordner **Quarantäne** oder **Backup**.

2. Im Arbeitsplatz des Ordners **Quarantäne** (**Backup**) wählen Sie mithilfe der Tasten **Umschalt** und **Strg** Dateien aus, die gelöscht werden sollen.

3. Löschen Sie die Dateien auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Dateien und wählen Sie **Entfernen** aus.
   - Klicken Sie auf den Link **Objekte löschen** (**Objekt löschen**, falls nur eine Datei gelöscht werden soll) im Block für die Bearbeitung der ausgewählten Dateien.

Daraufhin werden diese Dateien, die von den Schutzprogrammen in die Datenverwaltung der Client-Geräte verschoben wurden, aus der jeweiligen Datenverwaltung gelöscht.

Dateien aus der Datenverwaltung wiederherstellen

Um eine Datei aus der Quarantäne oder aus dem Backup wiederherzustellen, gehen Sie wie folgt vor:

1. In der Konsolenstruktur im Ordner **Datenverwaltung** öffnen Sie den Unterordner **Quarantäne** oder **Backup**.
2. Im Arbeitsplatz des Ordners **Quarantäne** (**Backup**) wählen Sie mithilfe der Tasten **Umschalt** und **Strg** Dateien aus, die wiederhergestellt werden sollen.
3. Starten Sie den Wiederherstellungsprozess der Dateien auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die betreffenden Dateien und wählen Sie **Wiederherstellen** aus.
   - Klicken Sie auf den Link **Wiederherstellen** im Bearbeitungsblock der ausgewählten Dateien.

Daraufhin werden diese Dateien, die von den Schutzprogrammen in die Datenverwaltung der Client-Geräte verschoben wurden, in den ursprünglichen Ordnern wiederhergestellt.

Datei aus der Datenverwaltung auf der Festplatte speichern

Kaspersky Security Center ermöglicht es, Kopien der Dateien auf dem Laufwerk zu speichern, die vom Schutzprogramm in die Quarantäne oder ins Backup des Client-Geräts verschoben wurden. Die Dateien werden auf das Gerät mit Kaspersky Security Center in den von Ihnen angegebenen Ordner kopiert.

Um eine Kopie der Datei aus der Quarantäne oder dem Backup zu speichern, gehen Sie wie folgt vor:

1. In der Konsolenstruktur im Ordner **Datenverwaltung** öffnen Sie den Unterordner **Quarantäne** oder **Backup**.

2. Im Arbeitsplatz des Ordners **Quarantäne** (**Backup**) wählen Sie eine Datei aus, die auf die Festplatte kopiert werden soll.

3. Starten Sie den Kopiervorgang der Datei auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Auf Datenträger speichern** aus.

   - Klicken Sie auf den Link **Auf Datenträger speichern** im Bearbeitungsblock der ausgewählten Datei.

Das Schutzprogramm, das die Datei in die Quarantäne auf dem Client-Gerät verschoben hat, speichert eine Kopie der Datei in dem vom Administrator angegebenen Ordner.

Untersuchung der Dateien in Quarantäne

Um Dateien zu untersuchen, die sich in Quarantäne befinden, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur im Ordner **Datenverwaltung** den Unterordner **Quarantäne**.

2. Im Arbeitsplatz des Ordners **Quarantäne** wählen Sie mithilfe der Tasten **Umschalt** und **Strg** Dateien, die untersucht werden sollen.

3. Starten Sie die Untersuchung für Dateien auf eine der folgenden Weisen:

- Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Objekte in der Quarantäne untersuchen** aus.
- Klicken Sie im Block mit den ausgewählten Dateien auf den Link **Untersuchen**.

Daraufhin wird für die Schutzprogramme, die Dateien in Quarantäne verschoben haben, eine Aufgabe zur Untersuchung auf Befehl auf den Client-Geräten gestartet, auf denen sich die in Quarantäne verschobenen Dateien befinden.

Dateien mit verschobener Verarbeitung

Informationen über Dateien mit verschobener Verarbeitung, die sich auf den Client-Geräten befinden, finden Sie im Ordner **Datenverwaltung** im Unterordner **Dateien mit verschobener Verarbeitung**.

Die verschobene Verarbeitung und die Desinfizierung von Dateien mithilfe des Schutzprogramms werden auf Befehl oder nach Eintreten eines bestimmten Ereignisses ausgeführt. Sie können Einstellungen der verschobenen Desinfizierung von Dateien anpassen.

Datei mit verschobener Verarbeitung desinfizieren

Um die Desinfizierung einer Datei mit verschobener Verarbeitung zu starten, gehen Sie wie folgt vor:

1. In der Konsolenstruktur im Ordner **Datenverwaltung** wählen Sie den Unterordner **Dateien mit verschobener Verarbeitung**.
2. Im Arbeitsplatz des Ordners **Dateien mit verschobener Verarbeitung** wählen Sie die Datei aus, die desinfiziert werden soll.
3. Starten Sie den Vorgang der Desinfizierung der Datei auf eine der folgenden Weisen:
   - Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Desinfizieren** aus.
   - Klicken Sie auf den Link **Desinfizieren** im Bearbeitungsblock der ausgewählten Datei.

Es wird daraufhin versucht, die Datei zu desinfizieren.

Wenn die Datei desinfiziert wurde, stellt das auf dem Client-Gerät installierte Schutzprogramm die Datei im ursprünglichen Ordner wieder her. Der Eintrag über die Datei wird aus dem Ordner **Dateien mit verschobener Verarbeitung** entfernt. Wenn eine Desinfizierung der Datei nicht möglich ist, löscht das auf dem Gerät installierte Schutzprogramm die Datei vom Gerät.
Der Eintrag über die Datei wird aus dem Ordner **Dateien mit verschobener Verarbeitung** entfernt.

Datei mit verschobener Verarbeitung auf Festplatte speichern

Kaspersky Security Center ermöglicht es, Kopien von Dateien mit verschobener Verarbeitung, die auf den Client-Geräten gefunden wurden, auf dem Laufwerk zu speichern. Die Dateien werden auf das Gerät mit Kaspersky Security Center in den von Ihnen angegebenen Ordner kopiert.

Um eine Kopie der Datei mit verschobener Verarbeitung auf der Festplatte zu speichern, gehen Sie wie folgt vor:

1. In der Konsolenstruktur im Ordner **Datenverwaltung** wählen Sie den Unterordner **Dateien mit verschobener Verarbeitung**.

2. Im Arbeitsplatz des Ordners **Dateien mit verschobener Verarbeitung** wählen Sie Dateien aus, die auf die Festplatte kopiert werden sollen.

3. Starten Sie den Kopiervorgang der Datei auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Auf Datenträger speichern** aus.

   - Klicken Sie auf den Link **Auf Datenträger speichern** im Bearbeitungsblock der ausgewählten Datei.

Daraufhin speichert das Schutzprogramm des Client-Geräts, auf dem die ausgewählte Datei mit verschobener Verarbeitung gefunden wurde, eine Kopie der Datei im angegebenen Ordner.

Dateien aus dem Ordner "Dateien mit verschobener Verarbeitung" löschen

*Um eine Datei aus dem Ordner **Dateien mit verschobener Verarbeitung** zu entfernen, gehen Sie wie folgt vor:*

1. In der Konsolenstruktur im Ordner **Datenverwaltung** wählen Sie den Unterordner **Dateien mit verschobener Verarbeitung**.

2. Im Arbeitsplatz des Ordners **Dateien mit verschobener Verarbeitung** wählen Sie mithilfe der Tasten **Umschalt** und **Strg** Dateien aus, die gelöscht werden sollen.

3. Löschen Sie die Dateien auf eine der folgenden Weisen:

   - Klicken Sie mit der rechten Maustaste auf die Dateien und wählen Sie **Entfernen** aus.

   - Klicken Sie auf den Link **Objekte löschen** (**Objekt löschen**, falls nur eine Datei gelöscht werden soll) im Block für die Bearbeitung der ausgewählten Dateien.

Daraufhin werden diese Dateien, die von den Schutzprogrammen in die Datenverwaltung der Client-Geräte verschoben wurden, aus der jeweiligen Datenverwaltung gelöscht. Einträge über die Dateien werden aus der Liste im Ordner **Dateien mit verschobener Verarbeitung** entfernt.

Kaspersky Security Network (KSN)

In diesem Abschnitt wird die Verwendung der Infrastruktur der Online-Dienste von Kaspersky Security Network (KSN) beschrieben. Er enthält Informationen über KSN sowie Anleitungen zur Aktivierung von KSN, zur Konfiguration des Zugriffs auf KSN und über die Statistiken der Verwendung des KSN-Proxyservers.

Über KSN

Das Kaspersky Security Network (KSN) ist eine Infrastruktur von Online-Diensten, die Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab bietet, in der Informationen über die Reputation der Dateien, Web-Ressourcen und Programme enthalten sind. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Lab-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. KSN ermöglicht den Abruf von Informationen über die auf den verwalteten Client-Geräten installierten Programme aus den Kaspersky-Lab-Reputations-Datenbanken.

Mit der Teilnahme an KSN stimmen Sie gemäß der KSN-Vereinbarung zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Lab-Programme, die von Kaspersky Security Center verwaltet werden, automatisch an Kaspersky Lab übertragen werden. Die Übertragung von Informationen erfolgt gemäß den konfigurierten Einstellungen für den Zugriff auf KSN (s. Abschnitt "Zugriff auf KSN einrichten" auf S. 369).

Das Programm empfiehlt, während der Programminstallation und während der Ausführung des Schnellstartassistenten eine Verbindung zu KSN herzustellen (s. Abschnitt "Schnellstartassistent für den Administrationsserver" auf S. 75). Sie können während der Ausführung des Programms jederzeit mit der Verwendung von KSN beginnen oder auf KSN verzichten (s. Abschnitt "KSN aktivieren und deaktivieren" auf S. 371).

Vom Administrationsserver verwaltete Client-Geräte interagieren mithilfe des KSN-Proxyservers mit KSN. Der Dienst des KSN-Proxyservers bietet folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren und an KSN Informationen übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen.
- Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Die Einstellungen des KSN Proxyservers können Sie im Abschnitt **KSN Proxyserver** im Eigenschaftenfenster des Administrationsservers ändern (s. Abschnitt "Zugriff auf KSN einrichten" auf S. 369).

Über die Bereitstellung von Daten

Mit der Teilnahme an Kaspersky Security Network stimmen Sie zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Lab-Programme, die von Kaspersky Security Center verwaltet werden, automatisch an Kaspersky Lab übertragen werden. Die Experten von Kaspersky Lab verwenden die von den Client-Geräten erhaltenen Informationen zur Beseitigung von Problemen bei der Ausführung der Kaspersky-Lab-Programme bzw. zur Veränderung ihrer Funktionalität.

Wenn Sie an Kaspersky Security Network teilnehmen, stimmen Sie zu, dass folgende Daten, die bei der Nutzung von Kaspersky Security Center auf dem Gerät gesammelt wurden, automatisch an Kaspersky Lab übermittelt werden:

- Name, Version, verwendete Sprache der Software, für die ein Update installiert wird
- Datenbankversion der Updates, die von der Software bei der Installation verwendet wird
- Ergebnis der Update-Installation
- Geräte-ID und Version des darauf verwendeten Administrationsagenten
- Software-Einstellungen, die bei der Installation der Updates verwendet wurden, etwa IDs der ausgeführten Vorgänge, Ergebniscodes der ausgeführten Vorgänge.

Falls Sie nicht am Programm Kaspersky Security Network teilnehmen, werden die oben angeführten Daten nicht an Kaspersky Lab übertragen.

Die erhaltenen Informationen werden von Kaspersky Lab gemäß den geltenden gesetzlichen Bestimmungen und bei Kaspersky Lab geltenden Regelungen geschützt. Die erhaltenen Daten werden von Kaspersky Lab ausschließlich in unpersönlicher Form sowie in Form einer allgemeinen Statistik verwendet. Die Daten der allgemeinen Statistik werden automatisch aus den gesammelten Quellinformationen ermittelt und enthalten keinerlei persönliche oder sonstige vertrauliche Daten. Die gesammelten Quellinformationen werden in verschlüsselter Form gespeichert und regelmäßig gelöscht (zweimal jährlich). Die Daten der allgemeinen Statistik werden unbegrenzt gespeichert.

Sämtliche Daten werden auf freiwilliger Basis zur Verfügung gestellt. Die Funktion, mit der die Daten zur Verfügung gestellt werden, kann zu jedem beliebigen Zeitpunkt im Fenster Programmeinstellungen aktiviert oder deaktiviert werden.

Zugriff auf KSN einrichten

Um den Zugriff des Administrationsservers auf KSN anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den Zugriff auf KSN angepasst werden soll.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN-Proxyserver** den Abschnitt **KSN Proxyserver-Einstellungen**.

4. Aktivieren Sie das Kontrollkästchen **Administrationsserver als Proxyserver verwenden**, um den Dienst des KSN-Proxyservers zu aktivieren.

   Die Übertragung von Daten der Client-Geräte an KSN wird durch die Richtlinie von Kaspersky Endpoint Security geregelt, die auf den Client-Geräten in Kraft ist. Wenn das Kontrollkästchen deaktiviert ist, findet keine Übertragung von Daten des Administrationsservers bzw. der Client-Geräte über Kaspersky Security Center an KSN statt. In diesem Fall können die Client-Geräte Daten entsprechend ihrer Einstellungen direkt an KSN übertragen (nicht über Kaspersky Security Center). Die auf den Client-

Geräten geltende Richtlinie für Kaspersky Endpoint Security für Windows bestimmt, welche Daten diese Geräte direkt (nicht über Kaspersky Security Center) an KSN senden.

5. Aktivieren Sie das Kontrollkästchen **Ich bin mit der Teilnahme an Kaspersky Security Network einverstanden**.

   Wenn dieses Kontrollkästchen aktiviert ist, werden die Ergebnisse der Installation von Patches von den Client-Geräten an Kaspersky Lab übermittelt. Wenn Sie das Kontrollkästchen aktivieren, müssen Sie die Bestimmungen der KSN-Vereinbarung lesen und akzeptieren.

   Wenn Sie ein Private KSN verwenden (die KSN-Infrastruktur befindet sich nicht auf den Servern von Kaspersky Lab sondern beispielsweise innerhalb des Netzwerks des Internetproviders), aktivieren Sie das Kontrollkästchen **Private KSN anpassen** und laden Sie mithilfe der Schaltfläche **Datei mit KSN-Einstellungen auswählen** die Einstellungen des Private KSN herunter (Dateien mit den Erweiterungen pkcs7, rem). Nach dem Herunterladen der Einstellungen werden in der Benutzeroberfläche die Bezeichnung des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit Einstellungen von Private KSN angezeigt.

   Die Arbeit mit Private KSN wird von den folgenden Kaspersky Lab-Programmen unterstützt:

   - Kaspersky Security Center 10 Service Pack 1 und höher
   - Kaspersky Endpoint Security 10 Service Pack 1 und höher
   - Kaspersky Security für Virtualisierung 3.0 Agentless Service Pack 2
   - Kaspersky Security für Virtualisierung 3.0 Service Pack 1 Light Agent.

   > Wenn Sie für die Arbeit mit Private KSN ältere Programmversionen als Kaspersky Security für Virtualisierung 3.0 Agentless Service Pack 2 oder Kaspersky Security für Virtualisierung 3.0 Service Pack 1 Light Agent verwenden, ist es empfehlenswert, die untergeordneten Administrationsserver zu verwenden, für die die Nutzung von Private KSN nicht konfiguriert ist.

6. Passen Sie die Einstellungen für die Verbindung des Administrationsservers mit dem Dienst des KSN-Proxyservers an:

- Geben Sie im Feld **TCP-Port** den TCP-Port an, über den die Verbindung zum KSN-Proxyserver aufgebaut werden soll. Standardmäßig erfolgt die Verbindung zum KSN-Proxyserver über Port 13111.

- Damit der Administrationsserver die Verbindung zum KSN-Proxyserver über einen UDP-Port herstellt, aktivieren Sie das Kontrollkästchen **UDP-Port verwenden** und geben Sie im Feld **UDP-Port** die Portnummer an. Standardmäßig ist das Kästchen deaktiviert und der Verbindungsaufbau zum KSN-Proxyserver erfolgt über UDP-Port 15111.

7. Aktivieren Sie das Kontrollkästchen**Untergeordneten Administrationsserver über den Hauptserver mit KSN verbinden**.

   Wenn das Kontrollkästchen aktiviert ist, verwenden die untergeordneten Administrationsserver den Hauptadministrationsserver als KSN-Proxyserver.
   Wenn das Kontrollkästchen deaktiviert ist, verbinden sich die untergeordneten Administrationsserver selbständig mit dem KSN. In diesem Fall verwenden die verwalteten Geräte die untergeordneten Administrationsserver als KSN-Proxyserver.

   > Die untergeordneten Administrationsserver verwenden den Hauptadministrationsserver als Proxyserver, wenn in den Eigenschaften der untergeordneten Administrationsserver im Abschnitt **KSN-Proxyserver** auch das Kontrollkästchen **Administrationsserver als Proxyserver verwenden** aktiviert ist.

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

Daraufhin werden die Einstellungen für den Zugriff auf KSN gespeichert.

KSN aktivieren und deaktivieren

Um KSN zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den KSN aktiviert werden soll.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN-Proxyserver** den Unterabschnitt **KSN Proxyserver-Einstellungen**.

4. Aktivieren Sie das Kontrollkästchen **Administrationsserver als Proxyserver verwenden**.

   Daraufhin wird der Dienst des KSN-Proxyservers aktiviert.

5. Aktivieren Sie das Kontrollkästchen **Ich bin mit der Teilnahme an Kaspersky Security Network einverstanden**.

   Daraufhin wird KSN aktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, werden die Ergebnisse der Installation von Patches von den Client-Geräten an Kaspersky Lab übermittelt. Wenn Sie das Kontrollkästchen aktivieren, müssen Sie die Bestimmungen der KSN-Vereinbarung lesen und akzeptieren.

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

Um die KSN zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den KSN aktiviert werden soll.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN-Proxyserver** den Unterabschnitt **KSN Proxyserver-Einstellungen**.

4. Deaktivieren Sie das Kontrollkästchen **Administrationsserver als Proxyserver verwenden**, um den Dienst des KSN-Proxyservers zu deaktivieren, oder deaktivieren Sie das Kontrollkästchen **Ich bin mit der Teilnahme an Kaspersky Security Network einverstanden**.

   Ist das Kontrollkästchen deaktiviert, werden von den Client-Geräten keine Ergebnisse der Installation von Patches an Kaspersky Lab übermittelt.

   Wenn Sie Private KSN verwenden, deaktivieren Sie das Kontrollkästchen **Private KSN anpassen**.

   Daraufhin wird KSN deaktiviert.

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

KSN Proxyserver-Statistik anzeigen

Der *KSN-Proxyserver* ist ein Dienst, der die Interaktion zwischen der Infrastruktur Kaspersky Security Network und den Client-Geräten, die vom Administrationsserver verwaltet werden, gewährleistet.

Die Verwendung des KSN-Proxyservers bietet Ihnen folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren und an KSN Informationen übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen.
- Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Im Eigenschaftenfenster des Administrationsservers können Sie die Einstellungen des KSN-Proxyservers anpassen und statistische Daten über die Verwendung des KSN-Proxyservers anzeigen.

Um die KSN Proxyserver-Statistiken anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Administrationsserver aus, für den die KSN-Statistik angezeigt werden soll.

2. Klicken Sie mit der rechten Maustaste auf den Administrationsserver, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN-Proxyserver** den Abschnitt **KSN Proxyserver-Statistik**.

   In diesem Abschnitt wird die Statistik über den KSN-Proxyserver angezeigt. Führen Sie erforderlichenfalls zusätzliche Aktionen aus:

   - Aktualisieren Sie mithilfe der Schaltfläche **Aktualisieren** die Statistikdaten über die Verwendung des KSN-Proxyservers.

   - Exportieren Sie mithilfe der Schaltfläche **In Datei exportieren** Statistikdaten in eine csv-Datei.

   - Überprüfen Sie mithilfe der Schaltfläche **KSN-Verbindung überprüfen**, ob der Administrationsserver derzeit mit KSN verbunden ist.

4. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.

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. 21) 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).

Appendix

Diesem Abschnitt können Informationen entnommen werden, die den Hauptteil des Dokumentes erweitern.

In diesem Abschnitt

Zusatzoptionen

In diesem Abschnitt werden zusätzliche Funktionen von Kaspersky Security Center besprochen, die die Möglichkeiten einer zentralisierten Programmverwaltung auf Client-Geräten erweitern.

In diesem Abschnitt

Automatisierung der Programmfunktion von Kaspersky Security Center. Tool klakaut

Sie können den Betrieb von Kaspersky Security Center mithilfe des Hilfsprogramms klakaut automatisieren. Das Hilfsprogramm klakaut und das entsprechende Hilfssystem befinden sich im Kaspersky Security Center Installationsordner.

Eigenständige Benutzer

In Kaspersky Security Center besteht die Möglichkeit, den Administrationsagenten eines Client-Geräts bei einer Änderung der folgenden Netzwerkeigenschaften auf andere Administrationsserver umzuschalten:

- Subnetz – Änderung der Adresse und Subnetzmaske
- DNS-Domäne – Änderung des DNS-Suffixes im Subnetz
- Adresse für Standard-Gateway – Änderung des Standard-Gateways im Netzwerk
- Adresse des DHCP-Servers – Änderung der IP-Adresse für den DHCP-Server im Netzwerk
- Adresse des DNS-Servers – Änderung der IP-Adresse für den DNS-Server im Netzwerk
- Adresse des WINS-Servers – Änderung der IP-Adresse für den WINS-Server im Netzwerk
- Verfügbarkeit der Windows-Domäne – Änderung des Status für die Windows-Domäne, mit der das Client-Gerät verbunden ist.

Die Funktionalität wird für die folgenden Betriebssysteme unterstützt: Microsoft Windows XP / Windows Vista; Microsoft Windows Server 2003 / 2008.

Bei der Installation des Administrationsagenten werden die ursprünglichen Verbindungseinstellungen des Administrationsagenten mit dem Server eingegeben. Sobald die Regeln für die Umstellung des Administrationsagenten mit anderen Administrationsservern definiert wurden, reagiert der Agent auf die Änderungen der Netzwerkeigenschaften folgendermaßen:

- Wenn die Netzwerkeigenschaften einer der erstellten Regeln entsprechen, wird der Administrationsagent mit dem in der Regel vorgegebenen Administrationsserver verbunden. Wenn dies durch die Regel vorgegeben wurde, gelten für die auf den Client-Geräten installierten Anwendungen mobile Richtlinien.
- Wird keine Regel ausgeführt, wird der Administrationsagent auf die ursprünglichen Verbindungseinstellungen mit dem Administrationsserver zurückgesetzt, die bei der Installation vorgegeben wurden. Die auf den Client-Geräten installierten Programme werden auf die aktiven Richtlinien zurückgesetzt.
- Ist der Administrationsserver nicht verfügbar, verwendet der Administrationsagent mobile Richtlinien.

> Standardmäßig wechselt der Administrationsagent zur mobilen Richtlinie, wenn der Administrationsserver seit mehr als 45 Minuten nicht verfügbar ist.

Die Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver werden im Verbindungsprofil gespeichert. Im Verbindungsprofil können Sie Regeln für den Wechsel der Client-Geräte zu mobilen Richtlinien erstellen sowie das Profil so einrichten, dass es nur zum Download von Updatedateien verwendet wird.

In diesem Abschnitt

Erstellung eines Verbindungsprofils zum Administrationsserver für eigenständige Benutzer

Um ein Verbindungsprofil des Administrationsagenten zum Administrationsserver für eigenständige Benutzer zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe, für deren Geräte ein Profil für die Verbindung des Administrationsagenten zum Server erstellt werden soll.

2. Führen Sie eine der folgenden Aktionen aus:

   - Um ein Verbindungsprofil für alle Geräte der Gruppe zu erstellen, wählen Sie im Arbeitsplatz in der Registerkarte **Richtlinien** die Richtlinie des Administrationsagenten aus. Öffnen Sie das Eigenschaftenfenster der ausgewählten Richtlinie.

   - Um ein Verbindungsprofil für ein bestimmtes Gerät innerhalb der Gruppe zu erstellen, wählen Sie im Arbeitsplatz in der Registerkarte **Geräte** das entsprechende Gerät aus und gehen Sie wie folgt vor:

     a. Öffnen Sie das Eigenschaftenfenster des ausgewählten Geräts.

     b. Wählen Sie im Eigenschaftenfenster des Geräts im Abschnitt **Programme** den erforderlichen Administrationsagenten aus.

     c. Öffnen Sie das Eigenschaftenfenster des Administrationsagenten.

3. Klicken Sie im folgenden Eigenschaftenfenster im Abschnitt **Netzwerk** auf den Unterabschnitt **Verbindung**.

4. Klicken Sie im Block **Profile für Verbindung mit Administrationsserver** auf die Schaltfläche **Hinzufügen**.

   Standardmäßig enthält die Liste der Verbindungsprofile nur das Profil <Ohne Verbindung>. Dieses Profil kann nicht geändert oder gelöscht werden. Es ist kein Server für eine Verbindung darin angegeben, und beim Wechsel zu diesem Profil versucht der Administrationsagent nicht, eine Verbindung zu einem Server aufzubauen. Die auf den Client-Geräten installierten Programme verwenden die mobilen Richtlinien. Das Profil <Ohne Verbindung> wird übernommen, wenn die Geräte vom Netzwerk getrennt sind.

5. Im geöffneten Fenster **Neues Profil** passen Sie die Einstellungen des Verbindungsprofils an und aktivieren Sie das Kontrollkästchen **Eigenständige Richtlinien aktivieren**.

Nach Aktivierung des Kontrollkästchens wird ein Verbindungsprofil des Administrationsagenten zum Administrationsserver für eigenständige Benutzer erstellt. Wird eine Verbindung des Administrationsagenten zum Server über dieses Profil hergestellt, so verwenden die auf dem Client-Gerät installierten Programme mobile Richtlinien.

Regel für die Umstellung des Administrationsagenten erstellen

Um eine Regel für die Umstellung des Administrationsagenten von einem Administrationsserver auf einen anderen Administrationsserver bei geänderten Eigenschaften des Netzwerks anzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur eine Administrationsgruppe, für deren Geräte eine Regel für die Umstellung des Administrationsagenten erstellt werden soll.

2. Führen Sie eine der folgenden Aktionen aus:

   - Um eine Regel für alle Geräte der Gruppe zu erstellen, wählen Sie im Arbeitsplatz der Gruppe in der Registerkarte **Richtlinien** die Richtlinie des Administrationsagenten aus. Öffnen Sie das Eigenschaftenfenster der ausgewählten Richtlinie.

   - Um eine Regel für ein bestimmtes Gerät innerhalb der Gruppe zu erstellen, wählen Sie im Arbeitsplatz in der Registerkarte **Geräte** das entsprechende Gerät aus und gehen Sie wie folgt vor:

     a. Öffnen Sie das Eigenschaftenfenster des ausgewählten Geräts.

     b. Wählen Sie im Eigenschaftenfenster des Geräts im Abschnitt **Programme** den erforderlichen Administrationsagenten aus.

     c. Öffnen Sie das Eigenschaftenfenster des Administrationsagenten.

3. Klicken Sie im folgenden Eigenschaftenfenster im Abschnitt **Netzwerk** auf den Unterabschnitt **Verbindung**.

4. Im Block **Profile wechseln** klicken Sie auf die Schaltfläche **Hinzufügen**.

5. Passen Sie im folgenden Fenster **Neue Regel** die Einstellungen für die Regeln der Umstellung an und aktivieren Sie das Kontrollkästchen **Regel aktiviert**, um die Verwendung der Regel zu aktivieren.

Nach der Regelaktivierung wird eine Umstellungsregel erstellt, bei deren Ausführung der Administrationsagent für die Verbindung mit dem Administrationsserver das in der Regel angegebene Verbindungsprofil verwenden wird.

Die Regeln für die Umstellung werden in der Reihenfolge, in der sie in der Liste aufgeführt sind, auf Übereinstimmung mit den Netzwerkeigenschaften überprüft.
Wenn die Netzwerkeigenschaften mehreren Regeln entsprechen, wird die erste Regel übernommen. Sie können die Reihenfolge der Regeln in der Liste mithilfe der Schaltflächen  und  ändern.

Ereignisse während der Programmausführung

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über die Ereignisse des Administrationsservers und anderer Kaspersky-Lab-Programme, die auf den Client-Geräten installiert sind.

Für Kaspersky-Lab-Programme sind vier Ereigniskategorien für Ereignisse vorgesehen:

- **Kritisches Ereignis**
- **Funktionsfehler**
- **Warnung**
- **Infomeldung**.

Sie können Regeln für die Bearbeitung von Ereignissen für jede Ereigniskategorie einzeln konfigurieren.

Siehe auch:

Allgemeine Einstellungen des Administrationsservers konfigurieren 105

Ereigniskategorie für die Überschreitung der Lizenzbeschränkung bestimmen

Kaspersky Security Center ermöglicht das automatische Empfangen von Informationen über Ereignisse der Überschreitung der Lizenzbeschränkung von Kaspersky-Lab-Programmen, die auf den Client-Geräten installiert sind.

Die Ereigniskategorie für die Überschreitung der Lizenzbeschränkung wird anhand folgender Regeln bestimmt:

- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz zwischen 90% und 100% der Gesamtmenge der Lizenzeinheiten dieser Lizenz liegt, wird das Ereignis in der Ereigniskategorie **Infomeldung** veröffentlicht.
- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz zwischen 100% und 110% der Gesamtmenge der Lizenzeinheiten dieser Lizenz liegt, wird das Ereignis in der Ereigniskategorie **Warnung** veröffentlicht.
- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz 110% der Gesamtmenge der Lizenzeinheiten dieser Lizenz übersteigt, wird das Ereignis in der Ereigniskategorie **Kritisches Ereignis** veröffentlicht.

Siehe auch:

Allgemeine Einstellungen des Administrationsservers konfigurieren 105

Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei

Kaspersky Security Center bietet die Möglichkeit, den Administrator durch den Start einer ausführbaren Datei über Ereignisse auf den Client-Geräten zu benachrichtigen. Diese ausführbare Datei muss eine weitere ausführbare Datei mit Parameterplatzhaltern für das Ereignis enthalten, die dem Administrator übermittelt werden müssen.

Tabelle 4. Parameterplatzhalter zur Beschreibung des Ereignisses

Parameterplatzhalter	Beschreibung des Parameterplatzhalters
%SEVERITY%	Ereigniskategorie des Ereignisses
%COMPUTER%	Name des Geräts, auf dem das Ereignis eingetreten ist
%DOMAIN%	Domäne
%EVENT%	Ereignis
%DESCR%	Ereignisbeschreibung
%RISE_TIME%	Zeitpunkt des Auftretens
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Aufgabenname
%KL_PRODUCT%	Kaspersky Security Center Administrationsagent
%KL_VERSION%	Versionsnummer des Administrationsagenten
%HOST_IP%	IP-Adresse
%HOST_CONN_IP%	IP-Adresse der Verbindung

Beispiel

Ausführbare Datei zur Benachrichtigung über Ereignisse (z. B. *script1.bat*), innerhalb der eine weitere ausführbare Datei (z. B. *script2.bat*) mit dem Parameterplatzhalter %COMPUTER% gestartet wird. Beim Auftreten eines Ereignisses auf dem Gerät des Administrators wird die Datei *script1.bat* gestartet, die wiederum die Datei *script2.bat* mit dem Parameter %COMPUTER% startet. Dadurch erhält der Administrator den Namen des Geräts, auf dem das Ereignis aufgetreten ist.

Arbeit mit dem Programm Kaspersky Security für Virtualisierung

Kaspersky Security Center unterstützt die Möglichkeit, virtuelle Maschinen mit dem Administrationsserver zu verbinden. Die Verwaltung von virtuellen Maschinen erfolgt mit dem Programm Kaspersky Security für Virtualisierung 3.0. Für weitere Details siehe: Administratorhandbuch für Kaspersky Security für Virtualisierung 3.0.

Status des Antiviren-Schutzes mit Systemregistrierung verfolgen

Gehen Sie wie folgt vor, um den Status des Antiviren-Schutzes auf dem Client-Gerät mithilfe der Informationen zu verfolgen, die vom Administrationsagenten in der Systemregistrierung gespeichert wurden:

1. Öffnen Sie die Systemregistrierung des Client-Geräts (z. B. lokal mit dem Befehl regedit im Menü **Start** → **Ausführen**).

2. Rufen Sie den folgenden Abschnitt auf:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103
   \1.0.0.0\Statistics\AVState
   ```

   In der Systemregistrierung werden Informationen über den Status des Antiviren-Schutzes des Client-Geräts angezeigt.

Der Status des Antiviren-Schutzes entspricht den Schlüsselwerten der unten stehenden Tabelle.

Tabelle 5. Registrierungsschlüssel und ihre möglichen Werte

Schlüssel (Datentyp)	Wert	Beschreibung
`Protection_AdmServer (REG_SZ)`	<Name des Administrationsservers>	Name des Administrationsservers, der das Gerät verwaltet.
`Protection_AvInstalled (REG_DWORD)`	Ungleich 0	Auf dem Gerät ist ein Schutzprogramm installiert.
`Protection_AvRunning (REG_DWORD)`	Ungleich 0	Der Echtzeitschutz des Geräts ist aktiv.
`Protection_HasRtp (REG_DWORD)`	Ungleich 0	Die Komponente Echtzeitschutz ist installiert.
	Status des Echtzeitschutzes:	
	0	Unbekannt
	2	Aus
	3	Angehalten
	4	Wird gestartet
	5	Ein
	6	An, hoch (maximale Sicherheit)
	7	An, Standardeinstellungen (empfohlen)
	8	An, Benutzereinstellungen
	9	Absturz

Schlüssel (Datentyp)	Wert	Beschreibung
`Protection_LastFscan (REG_SZ)`	TT-MM-JJJJ HH-MM-SS	Datum und Uhrzeit (UTC-Format) der letzten vollständigen Untersuchung
`Protection_BasesDate (REG_SZ)`	TT-MM-JJJJ HH-MM-SS	Erscheinungsdatum und -Uhrzeit (im UTC-Format) der Programm-Datenbanken
`Protection_LastConnected (REG_SZ)`	TT-MM-JJJJ HH-MM-SS	Datum und Uhrzeit (UTC-Format) der letzten Herstellung einer Verbindung mit dem Administrationsserver

Server-Cluster und -Arrays

Kaspersky Security Center unterstützt die Cluster-Technologie. Sobald der Administrationsserver vom Administrationsagenten die Information erhält, dass ein auf einem Client-Gerät installiertes Programm zum Server-Array gehört, wird das betreffende Client-Gerät als Knoten in den Cluster eingebunden. Der Cluster wird als separates Objekt in der Konsolenstruktur im Ordner **Verwaltete Geräte** mit dem Symbol  hinzugefügt (s. Abb. unten).

Cluster weisen folgende typische Merkmale auf:

- Ein Cluster und alle seine Knoten befinden sich stets in derselben Administrationsgruppe.
- Versucht der Administrator, einen Knoten eines Clusters zu verschieben, kehrt dieser automatisch wieder an seine ursprüngliche Position zurück.
- Versucht der Administrator, einen Knoten eines Clusters in eine andere Gruppe zu verschieben, so werden sämtliche Knoten des Clusters in die betreffende Gruppe verschoben.

Algorithmus der Installation des Patches für ein Kaspersky-Lab-Programm im Cluster-Modell

Kaspersky Security Center unterstützt nur die manuelle Installation von Patches für Kaspersky-Lab-Programme im Cluster-Modell.

Um einen Patch für ein Kaspersky-Lab-Programm zu installieren, gehen Sie wie folgt vor:

1. Laden Sie den Patch auf jeden Knoten des Clusters.
2. Starten Sie die Installation des Patches auf dem aktiven Knoten.

   Warten Sie die erfolgreiche Installation des Patches ab.
3. Starten Sie den Patch auf allen untergeordneten Knoten des Clusters der Reihe nach.

   Wenn Sie den Patch aus der Befehlszeile starten, verwenden Sie den Schlüssel "`-CLUSTER_SECONDARY_NODE`".

   Als Resultat der Ausführung dieser Aktionen wird der Patch auf jedem Knoten des Clusters installiert.
4. Führen Sie die Cluster-Dienste von Kaspersky Lab manuell aus.

Jeder Knoten des Clusters wird in der Verwaltungskonsole als Gerät mit installiertem Administrationsagenten angezeigt.

Informationen über die installierten Patches finden Sie im Ordner **Software-Updates** oder im Bericht über die Update-Versionen der Programm-Module der Kaspersky-Lab-Programme.

Siehe auch:

Allgemeine Einstellungen des Administrationsservers konfigurieren 105

Suche nach Geräten

Kaspersky Security Center ermöglicht eine Suche der Geräte auf der Grundlage der angegebenen Kriterien. Suchergebnisse können in einer Textdatei gespeichert werden.

Mit der Suchfunktion können folgende Geräte gefunden werden:

- Client-Geräte der Administrationsgruppen des Administrationsservers und seiner untergeordneten Server
- nicht zugeordnete Geräte unter der Verwaltung des Administrationsservers und seiner untergeordneten Server.

Um die Suche von Client-Geräten einer Administrationsgruppe auszuführen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner der Administrationsgruppe aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner der Administrationsgruppe und wählen Sie **Suchen** aus.
3. Geben Sie auf den Registerkarten des Fensters **Suchen** die Kriterien an, nach denen die Client-Geräte gesucht werden sollen, und klicken Sie auf die Schaltfläche **Suchen**.

Daraufhin werden die Geräte, die den angegebenen Suchkriterien entsprechen, in der Tabelle im unteren Bereich des Fensters **Suchen** angezeigt.

Für die Suche von nicht zugeordneten Geräten gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Nicht zugeordnete Geräte** aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Nicht zugeordnete Geräte** und wählen Sie **Suchen** aus.
3. Geben Sie auf den Registerkarten des Fensters **Suchen** die Kriterien an, nach denen die Client-Geräte gesucht werden sollen, und klicken Sie auf die Schaltfläche **Suchen**.

Daraufhin werden die Geräte, die den angegebenen Suchkriterien entsprechen, in der Tabelle im unteren Bereich des Fensters **Suchen** angezeigt.

Um Geräte unabhängig davon zu suchen, ob sie einer Administrationsgruppe zugeordnet wurden oder nicht, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Administrationsserver – <Servername>**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten und wählen Sie **Suchen** aus.
3. Geben Sie auf den Registerkarten des Fensters **Suchen** die Kriterien an, nach denen die Client-Geräte gesucht werden sollen, und klicken Sie auf die Schaltfläche **Suchen**.

Daraufhin werden die Geräte, die den angegebenen Suchkriterien entsprechen, in der Tabelle im unteren Bereich des Fensters **Suchen** angezeigt.

> Außerdem können Sie im Fenster **Suchen** mithilfe der Dropdown-Liste, die sich in der rechten oberen Ecke des Fensters befindet, Administrationsgruppen und untergeordnete Administrationsserver suchen. Die Suche nach Administrationsgruppen und untergeordneten Administrationsservern kann nicht über das Fenster **Suchen** im Ordner **Nicht zugeordnete Geräte** ausgeführt werden.

Zur Suche nach Geräten können Sie in den Eingabefeldern des Fensters **Suchen** regulären Ausdrücke (s. Abschnitt "Reguläre Ausdrücke in der Suchzeile verwenden" auf S. 434) verwenden.

Die Volltextsuche im Fenster **Suchen** ist verfügbar:

- auf der Registerkarte **Netzwerk** im Feld **Kommentar**
- auf der Registerkarte **Hardware** in den Feldern **Gerät**, **Hersteller**, **Beschreibung**.

Verbindung mit den Client-Geräten über Windows Desktopfreigabe herstellen

Um eine Verbindung mit einem Gerät über Windows Desktopfreigabe herzustellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur auf der Registerkarte **Geräte** den Ordner **Verwaltete Geräte** aus.

   Im Arbeitsplatz des Ordners wird eine Liste der Geräte angezeigt.

2. Klicken Sie mit der rechten Maustaste auf das Client-Gerät, mit dem Sie eine Verbindung herstellen möchten, und wählen Sie im Kontextmenü **Mit Gerät verbinden** → **Windows Desktopfreigabe** aus.

   Das Fenster **Desktopsitzung auswählen** wird geöffnet.

3. Wählen Sie im Fenster **Desktopsitzung auswählen** eine Desktopsitzung aus, die zum Herstellen einer Verbindung mit dem Gerät verwendet werden soll.

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

Es wird eine Verbindung mit dem Gerät hergestellt.

Über verwendete Benutzerkonten

Sie können ein Benutzerkonto festlegen, unter dem eine Aufgabe gestartet werden soll.

Zum Beispiel sind zur Ausführung von Aufgaben zur Untersuchung auf Befehl Zugriffsrechte auf das zu untersuchende Objekt erforderlich, und zur Ausführung von Update-Aufgaben Zugriffsrechte für den autorisierten Proxyserver-Benutzer. Das Festlegen eines Benutzerkontos für den Aufgabenstart ermöglicht es, Fehler bei der Ausführung der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe zu vermeiden, wenn der Benutzer, der eine Aufgabe gestartet hat, nicht über die entsprechenden Zugriffsrechte verfügt.

In den Aufgaben zur Remote-Installation und -Deinstallation des Programms wird ein Benutzerkonto für den Download der (de)installationsrelevanten Dateien auf die Client-Geräte verwendet, wenn auf dem Gerät der Administrationsagent nicht installiert oder nicht verfügbar ist. Beim installierten und verfügbaren Administrationsagenten wird das Benutzerkonto verwendet,

wenn die Bereitstellung der Dateien gemäß den Aufgabeneinstellungen nur mit Microsoft Windows-Funktionen aus dem freigegebenen Ordner erfolgt. In diesem Fall muss das Benutzerkonto auf dem Client-Gerät über folgende Berechtigungen verfügen:

- Recht auf Remote-Start von Anwendungen
- Rechte für die Ressource Admin$
- Recht *Als Dienst anmelden*.

Wenn der Administrationsagent die Dateien für Client-Geräte bereitstellt, wird das Benutzerkonto nicht verwendet. Alle Kopiervorgänge und die Installation der Dateien erledigt der Administrationsagent unter dem Benutzerkonto **Lokales System** (**Local System Account**).

Arbeiten mit externen Instrumenten

Mithilfe von Kaspersky Security Center lässt sich eine Liste von *externen Werkzeugen* (im Weiteren auch *Tools*) erstellen. Das sind Programme, die für das Client-Gerät aus der Verwaltungskonsole mithilfe der Kontextmenü-Gruppe **Externe Tools** aufgerufen werden. Zu jedem Element der Tool-Liste wird ein separater Menüeintrag angelegt, mit dem die Verwaltungskonsole das dem Tool entsprechende Programm startet.

Das Programm wird im Administrator-Arbeitsplatz gestartet. Es kann als Argumente der Befehlszeile Attribute des Remote-Client-Geräts (NetBIOS-Name, DNS-Name, IP-Adresse) entgegennehmen. Die Verbindung zum Remote-Gerät kann über eine getunnelte Verbindung erfolgen.

Standardmäßig sind für jedes Client-Gerät auf der Liste mit externen Tools die folgenden Dienstprogramme verfügbar:

- **Remote-Diagnose** – Ferndiagnosetool von Kaspersky Security Center.
- **Remote-Desktop** – Standardkomponente von Microsoft Windows "Remotedesktopverbindung"
- **Computerverwaltung** – Standardkomponente von Microsoft Windows.

Um externe Tools hinzuzufügen oder zu löschen sowie ihre Einstellungen anzupassen,

klicken Sie mit der rechten Maustaste auf das gewünschte Client-Gerät und wählen Sie **Externe Tools** → **Externe Tools konfigurieren** aus.

Das Fenster **Externe Tools** öffnet sich. In diesem Fenster können Sie externe Tools hinzufügen, löschen oder ihre Einstellungen anpassen mithilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Entfernen**.

Listen aus Dialogfenstern exportieren

In den Dialogfenstern des Programms können Sie Objektlisten in Textdateien exportieren.

Objektlisten können nur für die Abschnitte des Dialogfensters exportiert werden, in welchen die Schaltfläche **In Datei exportieren** vorhanden ist.

Laufwerk klonen-Modus des Administrationsagenten

Das Klonen der Festplatte eines Referenzgerätes ist eine verbreitete Methode zur Installation von Software auf neuen Geräten. Wenn der Administrationsagent auf der Festplatte des Referenzgerätes während des Klonens im Standardmodus ausgeführt wird, kann das folgende Problem auftreten:

Nach der Verteilung des Referenz-Image der Festplatte mit dem Administrationsagenten auf den neuen Geräten werden diese Geräte in der Verwaltungskonsole mit dem gleichen Symbol dargestellt. Das Problem tritt auf, weil beim Klonen auf den neuen Geräten identische interne Daten gespeichert werden, die es dem Administrationsserver erlauben, das Gerät mit dem Symbol in der Verwaltungskonsole zu verknüpfen.

Die Probleme mit der inkorrekten Anzeige neuer Geräte in der Verwaltungskonsole nach dem Klonen können mithilfe des speziellen *Laufwerk klonen-Modus des Administrationsagenten* vermieden werden. Verwenden Sie diesen Modus, wenn Sie die Software (mit dem Administrationsagenten) auf neuen Geräten mittels der Laufwerk klonen-Methode verteilen.

Im Laufwerk klonen-Modus wird der Administrationsagent ausgeführt, stellt aber keine Verbindung mit Administrationsserver her. Beim Ausschalten des Laufwerk klonen-Modus löscht der Administrationsagent die internen Daten, aufgrund deren der Administrationsserver mehrere Geräte mit einem Symbol in der Verwaltungskonsole verknüpft. Nach Abschluss des Klonens des Referenzgerät-Image werden neue Geräte in der Verwaltungskonsole korrekt (als einzelne Symbole) angezeigt.

Handlungsempfehlung für das Laufwerkklonen des Administrationsagenten

1. Der Administrator installiert den Administrationsagenten auf dem Referenzgerät.
2. Der Administrator überprüft die Verbindung des Administrationsagenten mit dem Administrationsserver mithilfe des Dienstprogramms klnagchk (s. Abschnitt "Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk" auf S. 161).
3. Der Administrator aktiviert den Laufwerk klonen-Modus des Administrationsagenten.
4. Der Administrator installiert Software und Patches auf dem Gerät und führt eine beliebige Anzahl von Geräteneustarts aus.
5. Der Administrator nimmt das Klonen des Referenzgerät-Laufwerks auf beliebig vielen Geräten vor.
6. Für jede geklonte Kopie müssen folgende Bedingungen erfüllt sein:
    a. Der Gerätename wurde geändert
    b. Das Gerät wurde neu gestartet
    c. Das Laufwerk klonen-Modus wurde deaktiviert.

Laufwerk klonen-Modus mithilfe des Dienstprogramms klmover aktivieren und deaktivieren

Um den Laufwerk klonen-Modus des Administrationsagenten zu aktivieren / deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie das Tool klmover auf dem Gerät mit dem installierten Administrationsagenten, das geklont werden soll.

   Das klmover-Dienstprogramm befindet sich im Installationsordner des Administrationsagenten.

2. Um den Laufwerk klonen-Modus zu aktivieren, geben Sie in der Windows-Befehlszeile den Befehl `klmover -cloningmode 1` ein.

   Der Administrationsagent schaltet in den Laufwerk klonen-Modus.

3. Um den aktuellen Status des Laufwerk klonen-Modus abzurufen, geben Sie in der Befehlszeile den Befehl `klmover -cloningmode` ein.

   Im Fenster des Dienstprogramms wird angezeigt, ob der Laufwerk klonen-Modus aktiviert oder deaktiviert ist.

4. Um den Laufwerk klonen-Modus zu deaktivieren, geben Sie in der Dienstprogramm-Befehlszeile den Befehl `klmover -cloningmode 0` ein.

Ein Gerät mit dem Betriebssystem Linux für die Remote-Installation des Administrationsagenten vorbereiten

Um ein Gerät mit dem Betriebssystem Linux für die Remote-Installation des Administrationsagenten vorzubereiten, gehen Sie wie folgt vor:

1. Überprüfen Sie die Konfiguration des Geräts:

   a. Stellen Sie sicher, dass eine Verbindung zum Gerät über ein Client-Programm mit SSH möglich ist (z. B. PuTTY).

   Wenn Sie keine Verbindung zum Gerät herstellen können, öffnen Sie die Datei /etc/ssh/sshd_config und stellen Sie sicher, dass die folgenden Einstellungen die nachstehenden Werte besitzen:

- PasswordAuthentication – nein
- ChallengeResponseAuthentication – ja

Speichern Sie die Datei (bei Bedarf) und starten Sie den SSH-Dienst über den Befehl sudo service ssh restart neu.

b. Deaktivieren Sie das Kennwort der Sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

Verwenden Sie den Befehl sudo visudo, um die Konfigurationsdatei sudoers zu öffnen. Geben Sie in der geöffneten Datei Folgendes ein:
username ALL = (ALL) NOPASSWD: ALL. Name und Kennwort des Benutzerkontos werden bei der Verbindung mit dem Gerät verwendet.

c. Speichern und schließen Sie die Datei sudoers.

d. Stellen Sie erneut eine Verbindung zum Gerät über SSH her und stellen Sie mithilfe des Befehls sudo whoami sicher, dass der Dienst Sudo kein Kennwort abfragt.

2. Laden Sie das Installationspaket herunter und erstellen Sie es:

a. Stellen Sie sicher, dass Libc auf dem Gerät installiert ist: apt-get install libc6-i386

b. Laden Sie das Installationspaket des Administrationsagenten herunter.

c. Verwenden Sie folgende Dateien, um ein Paket für Remote-Installation zu erstellen:

- klnagent.kpd
- akinstall.sh
- klnagent_8.5.0-662_i386.deb

d. Vor dem Erstellen des Installationspakets ändern Sie in der Datei akinstall.sh die Zeile 81: MkDir -p "$ LogDir".

3. Erstellen Sie eine Aufgabe zur Remote-Installation des Programms mit den folgenden Einstellungen:

- Aktivieren Sie im Fenster **Einstellungen** des Assistenten zum Erstellen von Aufgaben das Kontrollkästchen **Durch das Betriebssystem mithilfe des Administrationsservers**. Deaktivieren Sie alle anderen Kontrollkästchen.

- Geben Sie im Fenster **Konto für die Ausführung der Aufgabe auswählen** die Einstellungen des Benutzerkontos an, das für die Verbindung mit dem Gerät über SSH verwendet werden.

4. Installieren Sie Network Emulator Toolkit.

   Nach Abschluss der Installation von Network Emulator Toolkit reduzieren Sie die Bandbreite des Kommunikationskanals auf dem Gerät auf 100 Kbit.

5. Starten Sie die Aufgabe zur Remote-Installation des Programms.

   Die Aufgabenausführung kann bis zu 20 Minuten dauern.

Verschieben ins Backup und Wiederherstellung der Daten des Administrationsservers

Das Verschieben von Daten ins Backup ermöglicht die Übertragung des Administrationsservers von einem Gerät auf einen anderen ohne Datenverlust. Mithilfe der Backup-Funktion können Sie Daten bei der Übertragung einer Datenbank des Administrationsservers auf ein anderes Gerät oder beim Wechsel zu einer neueren Version von Kaspersky Security Center wiederherstellen.

Sie können eine Sicherungskopie der Daten des Administrationsservers auf eine der folgenden Weisen erstellen:

- Aufgabe zum Verschieben von Daten ins Backup über die Verwaltungskonsole erstellen und starten.

- Tool klbackup auf einem Gerät mit dem installierten Administrationsserver starten. Dieses Tool gehört zum Lieferumfang von Kaspersky Security Center. Es befindet sich nach der Installation des Administrationsservers im Stammverzeichnis des Zielordners, der bei der Installation angegeben wurde.

In der Sicherungskopie der Daten des Administrationsservers werden folgende Daten gespeichert:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte
- Speicherort der Programmpakete für die Remote-Installation
- Zertifikat des Administrationsservers.

Die Wiederherstellung von Daten des Administrationsservers ist nur mithilfe des Hilfsprogramms klbackup möglich.

In diesem Abschnitt

Aufgabe zum Erstellen einer Sicherungskopie der Daten anlegen

Die Aufgabe zum Erstellen einer Sicherungskopie gehört zu den Aufgaben des Administrationsservers und wird vom Schnellstartassistenten erstellt.
Wenn die vom Schnellstartassistenten erstellte Aufgabe zum Sicherungskopieren gelöscht wurde, können Sie diese manuell erstellen.

Um eine Aufgabe zum Sicherungskopieren des Administrationsservers zu erstellen, gehen Sie wie folgt vor:

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

2. Starten Sie den Vorgang zum Erstellen der Aufgabe auf eine der folgenden Weisen:

   - Wählen Sie im Kontextmenü des Ordners **Aufgaben** der Konsolenstruktur den Punkt **Erstellen** → **Aufgabe** aus.

   - Klicken Sie im Arbeitsplatz auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet. Folgen Sie den Anweisungen. Wählen Sie im Fenster **Aufgabentyp** des Assistenten den Aufgabentyp **Sicherungskopie der Serverdaten erstellen** aus.

Die Aufgabe **Sicherungskopie der Serverdaten erstellen** kann nur einmal erstellt werden. Wenn die Aufgabe zum Sicherungskopieren des Administrationsservers für den Administrationsserver bereits erstellt wurde, wird sie im Fenster für die Auswahl des Aufgabentyps des Assistenten zum Erstellen einer Aufgabe nicht angezeigt.

Tool Sicherungskopie und Wiederherstellung der Daten (klbackup)

Sie können Daten des Administrationsservers für ein Backup und die nachfolgende Wiederherstellung mithilfe des Hilfsprogramms klbackup kopieren, das zum Lieferumfang von Kaspersky Security Center gehört.

Hilfsprogramm klbackup kann in zwei Modi arbeiten:

- interaktiv (s. Abschnitt "Verschieben ins Backup und Wiederherstellung von Daten im interaktiven Modus" auf S. 402);

- nicht interaktiv (s. Abschnitt "Verschieben ins Backup und Wiederherstellung von Daten im nicht interaktiven Modus" auf S. 404).

Verschieben ins Backup und Wiederherstellung von Daten im interaktiven Modus

Um eine Sicherungskopie der Daten des Administrationsservers im interaktiven Modus zu erstellen, gehen Sie wie folgt vor:

1. Starten Sie das Hilfsprogramm klbackup, das sich im Installationsordner von Kaspersky Security Center befindet.

   Der Assistent für das Verschieben ins Backup und die Wiederherstellung von Daten wird gestartet.

2. Wählen Sie im ersten Fenster des Assistenten den Punkt **Erstellen einer Sicherungskopie der Daten des Administrationsservers**.

   Bei aktiviertem Kontrollkästchen **Erstellen einer Sicherungskopie und Wiederherstellen nur für Zertifikat des Administrationsservers** wird nur die Backup-Kopie des Zertifikats des Administrationsservers gespeichert.

   Klicken Sie auf die Schaltfläche **Weiter**.

3. Im folgenden Fenster des Assistenten geben Sie das Kennwort und den Zielordner für Sicherungskopien an. Klicken Sie auf **Weiter**, um das Verschieben ins Backup zu starten.

Um Daten des Administrationsservers im interaktiven Modus wiederherzustellen, gehen Sie wie folgt vor:

1. Deinstallieren Sie den Administrationsserver und installieren Sie ihn sodann erneut.

2. Starten Sie das Hilfsprogramm klbackup, das sich im Installationsordner von Kaspersky Security Center befindet.

   Der Assistent für das Verschieben ins Backup und die Wiederherstellung von Daten wird gestartet.

   > Das Tool klbackup muss unter demselben Benutzerkonto gestartet werden, unter dem auch der Administrationsserver installiert worden ist.

3. Im ersten Fenster des Assistenten wählen Sie den Punkt **Wiederherstellen der Daten des Administrationsservers**.

   Bei aktiviertem Kontrollkästchen **Erstellen einer Sicherungskopie und Wiederherstellen nur für Zertifikat des Administrationsservers** wird nur das Zertifikat des Administrationsservers wiederhergestellt.

   Klicken Sie auf die Schaltfläche **Weiter**.

4. Gehen Sie im Assistenten im Fenster **Einstellungen für Wiederherstellung** folgendermaßen vor:

   - Geben Sie den Ordner an, der die Backup-Kopie der Daten des Administrationsservers enthält.
   - Geben Sie das Kennwort ein, das beim Verschieben ins Backup festgelegt wurde.

5. Klicken Sie auf die Schaltfläche **Weiter** für die Wiederherstellung von Daten.

   Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Anlegen der Sicherungskopie. Wenn das Kennwort nicht stimmt, werden die Daten nicht wiederhergestellt. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Ferninstallation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden.

   Während der Wiederherstellung von Daten aus der Sicherungskopie darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen.

Verschieben ins Backup und Wiederherstellung von Daten im nicht interaktiven Modus

Um eine Sicherungskopie der Daten zu erstellen oder Daten des Administrationsservers im nicht interaktiven Modus wiederherzustellen,

starten Sie aus der Befehlszeile des Geräts, auf dem der Administrationsserver installiert ist, das Tool klbackup mit der erforderlichen Auswahl an Schlüsseln.

Die Syntax des Tools lautet:

```
klbackup [-logfile LOGFILE] -path BACKUP_PATH [-use_ts]|[-
restore] -savecert PASSWORD
```

> Wenn in der Befehlszeile des Tools klbackup kein Kennwort eingegeben wird, fragt das Tool das Kennwort interaktiv ab.

Die Schlüssel weisen folgende Bedeutung auf:

- `-logfile LOGFILE` – Bericht über das Kopieren oder Wiederherstellen der Daten des Administrationsservers speichern.
- `-path BACKUP_PATH` – Daten im Ordner BACKUP_PATH speichern/zum Wiederherstellen Daten aus dem Ordner BACKUP_PATH (Pflichtparameter) verwenden.

  > Das Benutzerkonto der Server-Datenbank und das Tool klbackup müssen über die Berechtigung zum Ändern der Daten im Ordner BACKUP_PATH verfügen.

- `-use_ts` – Beim Speichern die Daten in einen Unterordner im Ordner BACKUP_PATH kopieren, dessen Name das aktuelle Systemdatum und die aktuelle Systemuhrzeit im Format `klbackup JJJJ-MM-TT # UU-MM-SS` enthält. Wenn der Schlüssel nicht eingegeben wurde, werden die Angaben im Stammverzeichnis des Ordners BACKUP_PATH abgelegt.

  > Wenn Sie versuchen, die Informationen in einem Ordner zu speichern, in dem bereits eine Backup-Kopie vorhanden ist, erscheint eine Fehlermeldung. Die Informationen werden nicht aktualisiert.

Mit dem Schlüssel `-use_ts` kann ein Datenarchiv des Administrationsservers angelegt werden. Wenn beispielsweise mit dem Schlüssel `-path der Ordner C:\KLBackups` vorgegeben wurde, werden im Ordner klbackup 2006-06-19 # 11-30-18 Informationen über den Status des Administrationsservers mit Stand vom 19. Juni 2006 um 11 Uhr, 30 Minuten und 18 Sekunden abgelegt.

- `-restore` – Daten des Administrationsservers wiederherstellen. Die Wiederherstellung der Daten erfolgt anhand der Informationen, die im Ordner BACKUP_PATH liegen. Wenn der Schlüssel fehlt, wird die Sicherungskopie im Ordner BACKUP_PATH erstellt.

- `-savecert PASSWORD` – Zertifikat des Administrationsservers speichern oder wiederherstellen. Für die Verschlüsselung und Entschlüsselung des Zertifikats wird das Kennwort verwendet, das mit dem Parameter PASSWORD vorgegeben wurde.

  Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Anlegen der Sicherungskopie. Wenn das Kennwort nicht stimmt, werden die Daten nicht wiederhergestellt. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Ferninstallation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden.

Während der Wiederherstellung von Daten aus der Sicherungskopie darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen.

Administrationsserver auf anderes Gerät übertragen

Um den Administrationsserver auf ein anderes Gerät zu übertragen, ohne die Datenbank des Administrationsservers wechseln zu müssen, gehen Sie wie folgt vor:

1. Erstellen Sie eine Sicherungskopie der Daten des Administrationsservers.

2. Installieren Sie den Administrationsserver auf dem ausgewählten Gerät.

   > Um das Übertragen der Administrationsgruppen zu vereinfachen, ist es wünschenswert, dass die Adresse des neuen Administrationsservers der Adresse des alten Servers entspricht. Die Adresse (Gerätename im Windows-Netzwerk oder IP-Adresse) ist in den Einstellungen für die Verbindung des Administrationsagenten mit dem Server angegeben.

3. Führen Sie auf dem neuen Administrationsserver das Wiederherstellen der Daten des Administrationsservers aus der Sicherungskopie aus.

4. Wenn die Adresse (Gerätename im Windows-Netzwerk oder IP-Adresse) des neuen Administrationsservers nicht mit der Adresse des vorherigen Servers übereinstimmt, erstellen Sie für die Anbindung der Client-Geräte zum neuen Server auf dem vorherigen Server eine Aufgabe zum Wechsel des Administrationsservers für die Gruppe **Verwaltete Geräte**.

   Wenn die Adressen übereinstimmen, muss keine Wechselaufgabe des Servers erstellt werden. In diesem Fall kann die Verbindung über die in den Einstellungen angegebene Serveradresse hergestellt.

5. Löschen Sie den vorherigen Administrationsserver.

Um den Administrationsserver auf ein anderes Gerät zu übertragen und die Datenbank des Administrationsservers dabei zu wechseln, gehen Sie wie folgt vor:

1. Erstellen Sie eine Sicherungskopie der Daten des Administrationsservers.

2. Installieren Sie einen neuen SQL-Server.

Damit die Datenbank korrekt auf den neuen Server übertragen wird, muss der SQL-Server dieselben Sortierschemata (Collation) wie der alte SQL-Server aufweisen.

3. Installieren Sie einen neuen Administrationsserver. Die Benennungen der Datenbanken des vorherigen und des neuen SQL-Servers müssen übereinstimmen.

   Um das Übertragen der Administrationsgruppen zu vereinfachen, ist es wünschenswert, dass die Adresse des neuen Administrationsservers der Adresse des alten Servers entspricht. Die Adresse (Gerätename im Windows-Netzwerk oder IP-Adresse) ist in den Einstellungen für die Verbindung des Administrationsagenten mit dem Server angegeben.

4. Führen Sie auf dem neuen Administrationsserver das Wiederherstellen der Daten des vorherigen Administrationsservers aus der Sicherungskopie aus.

5. Wenn die Adresse (Gerätename im Windows-Netzwerk oder IP-Adresse) des neuen Administrationsservers nicht mit der Adresse des vorherigen Servers übereinstimmt, erstellen Sie für die Anbindung der Client-Geräte zum neuen Server auf dem vorherigen Server eine Aufgabe zum Wechsel des Administrationsservers für die Gruppe **Verwaltete Geräte**.

6. Wenn die Adressen übereinstimmen, muss keine Wechselaufgabe des Servers erstellt werden. In diesem Fall kann die Verbindung über die in den Einstellungen angegebene Serveradresse hergestellt.

7. Löschen Sie den vorherigen Administrationsserver.

Verschieben ins Backup und Wiederherstellung von Daten im interaktiven Modus

Durch das Warten der Datenbanken des Administrationsservers kann deren Umfang verringert, sowie die Leistungsfähigkeit und die Zuverlässigkeit des Programms verbessert werden. Es wird empfohlen, die Datenbanken des Administrationsservers mindestens einmal pro Woche zu warten.

Das Warten der Datenbanken des Administrationsservers erfolgt mithilfe der entsprechenden Aufgaben. Während der Wartung der Datenbanken führt das Programm folgenden Aktionen aus:

- Datenbanken auf Fehler überprüfen
- Datenbanken neu indizieren
- Datenbankstatistik aktualisieren
- Datenbank komprimieren (falls erforderlich).

MySQL wird von der Aufgabe zur Wartung der Datenbanken des Administrationsservers nicht unterstützt. Wenn als DBMS MYSQL verwendet wird, muss der Administrator selbsttätig eine Wartung der Datenbanken durchführen.

Um eine Aufgabe zur Wartung der Datenbank des Administrationsservers zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten des Administrationsservers, für den eine Aufgabe zur Wartung der Datenbank erstellt werden soll.
2. Wählen Sie den Ordner **Aufgaben** aus.
3. Klicken Sie im Arbeitsplatz des Ordners **Aufgaben** auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird der Assistent zur Erstellung einer Aufgabe gestartet.
4. Wählen Sie im Fenster **Aufgabentyp auswählen** des Assistenten den Aufgabentyp **Datenbanken bedienen** und klicken Sie auf die Schaltfläche **Weiter**.
5. Wenn die Datenbank des Administrationsservers während der Wartung komprimiert werden muss, aktivieren Sie im Fenster **Einstellungen** des Assistenten das Kontrollkästchen **Datenbank komprimieren**.
6. Folgen Sie den weiteren Schritten des Assistenten.

Die erstellte Aufgabe wird in der Aufgabenliste im Arbeitsplatz des Ordners **Aufgaben** angezeigt. Für einen Administrationsserver kann nur eine Aufgabe zur Wartung der Datenbanken ausgeführt werden. Wenn für den Administrationsserver bereits eine Aufgabe zur Wartung der Datenbanken erstellt wurde, ist es nicht möglich, eine weitere Aufgabe zur Wartung von Datenbanken zu erstellen.

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.

Besonderheiten der Verwaltungsoberfläche

In diesem Abschnitt

Wie ein verschwundenes Eigenschaftenfenster wieder hergestellt wird

Manchmal verschwindet das geöffnete Eigenschaftenfenster eines Objektes vom Bildschirm. Das kommt vor, wenn das Eigenschaftenfenster vom Programmhauptfenster verdeckt wird. (Diese Situation tritt insbesondere bei Verwendung der Microsoft Management Console auf.)

Um zum verschwundenen Eigenschaftenfenster des Objekts zu wechseln,

drücken Sie die Tastenkombination **ALT**+**TAB**.

Wie in der Konsolenstruktur navigiert wird

Um in der Konsolenstruktur zu navigieren, können Sie in der Symbolleiste auf folgende Schaltflächen klicken:

-  – Um einen Schritt zurück;
-  – Um einen Schritt nach vorn;
-  – Um eine Ebene nach oben.

Außerdem können Sie die Navigationskette in der rechten oberen Ecke des Arbeitsplatzes verwenden. Die Navigationskette enthält den kompletten Pfad zum Ordner der Konsolenstruktur, in dem Sie sich gegenwärtig befinden. Mit Ausnahme des letzten Elements fungieren alle Elemente der Kette als Links auf die Objekte der Konsolenstruktur.

Wie das Eigenschaftenfenster eines Objekts im Arbeitsplatz geöffnet wird

Die Eigenschaften der meisten Objekte der Verwaltungskonsole lassen sich im Eigenschaftenfenster ändern.

Gehen Sie wie folgt vor, um das Eigenschaftenfenster eines Objekts im Arbeitsplatz zu öffnen:

- Öffnen Sie das Kontextmenü des Objekts, und wählen Sie **Eigenschaften** aus.
- Wählen Sie das Objekt aus, und drücken Sie die Tastenkombination **ALT**+**ENTER**.

Wie eine Gruppe von Objekten im Arbeitsplatz ausgewählt wird

Sie können eine Gruppe von Objekten im Arbeitsplatz auswählen. Mit einer Gruppe von Objekten können Sie beispielsweise bestimmte Geräte auswählen und Aufgaben für sie anlegen.

Gehen Sie wie folgt vor, um einen Objektbereich auszuwählen:

1. Wählen Sie das erste Objekt des Bereichs aus, und drücken Sie die Taste **Umschalt**.
2. Halten Sie die **Umschalt**taste gedrückt, und wählen Sie das letzte Objekt des Bereichs aus.

Dadurch wird der Bereich ausgewählt.

Um individuelle Objekte in einer Gruppe zusammenzufassen, gehen Sie wie folgt vor:

1. Wählen Sie das erste Objekt in der Gruppe aus, und drücken Sie die Taste **STRG**.
2. Halten Sie die Taste **STRG** gedrückt und wählen Sie die übrigen Objekte der Gruppe.

Dadurch werden die Objekte in einer Gruppe zusammengefasst.

Wie die Auswahl von Spalten im Arbeitsplatz geändert wird

In der Verwaltungskonsole können Sie die Auswahl an Spalten ändern, die im Arbeitsplatz angezeigt werden.

Um die Auswahl an Spalten im Arbeitsplatz zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur das Objekt aus, für das Sie die Spalten ändern wollen.
2. Wählen Sie im Menü der Verwaltungskonsole den Befehl **Ansicht** → **Spalten hinzufügen oder löschen**.
3. Legen Sie im folgenden Fenster die Spalten fest, die angezeigt werden sollen.

Hilfe

In diesem Abschnitt finden Sie eine tabellarische Übersicht zum Kontextmenü der Objekte der Verwaltungskonsole und zum Status der Objekte im Konsolenbaum und Arbeitsplatz.

In diesem Abschnitt

Update-Agenten als Gateway verwenden

Wenn der Administrationsserver zur demilitarisierten Zone (DMZ) nicht gehört, ist das Herstellen einer Verbindung zwischen den Administrationsagenten, die zur demilitarisierten Zone gehören, und dem Administrationsserver nicht möglich.

Zum Herstellen einer Verbindung zwischen dem Administrationsserver und den Administrationsagenten kann ein Update-Agent als Verbindungs-Gateway verwendet werden. Der Update-Agent stellt dem Administrationsserver den Port für den Verbindungsaufbau zur Verfügung. Der Administrationsserver stellt beim Starten eine Verbindung zum Update-Agenten her und trennt diese Verbindung während seines Betriebs nicht.

Nachdem der Update-Agent ein Signal des Administrationsservers empfangen hat, sendet der Update-Agent ein UDP-Signal an die Administrationsagenten zur Verbindung mit dem Administrationsserver. Nach Empfang des Signals werden die Administrationsagenten mit dem Update-Agenten verbunden, der Informationen zwischen den Administrationsagenten und dem Administrationsserver übermittelt.

Masken in Zeichenfolgenvariablen verwenden

Für Zeichenfolgenvariablen können Masken verwendet werden. Masken können Sie mit folgenden regulären Ausdrücken erstellen:

- * – beliebige Ausdrücke mit einer Länge von 0 oder mehr Symbolen
- ? – ein beliebiges Einzelsymbol
- [<Intervall>] – ein Symbol aus dem festgelegten Bereich bzw. der festgelegten Menge.

  Beispiel: [0–9] – beliebige Ziffer; [abcdef] – eines der Symbol a, b, c, d, e, f.

Befehle des Kontextmenüs

Dieser Abschnitt enthält ein Objektverzeichnis der Verwaltungskonsole und eine entsprechende Punkteauswahl des Kontextmenüs (siehe Tabelle unten).

Tabelle 6. Elemente des Kontextmenüs der Objekte in der Verwaltungskonsole

Objekt	Menüpunkt	Zweck des Menüpunkts
Allgemeine Einträge im Kontextmenü	**Suchen**	Fenster Suche nach Geräten öffnen
	Aktualisieren	Anzeige des ausgewählten Objekts aktualisieren
	Liste exportieren	Aktuelle Liste in Datei exportieren
	Eigenschaften	Eigenschaftenfenster des ausgewählten Objekts öffnen

Objekt	Menüpunkt	Zweck des Menüpunkts
	Ansicht → Spalten hinzufügen oder löschen	Spalten in der Objekttabelle im Arbeitsplatz hinzufügen oder löschen
	Ansicht → Große Symbole	Objekte im Arbeitsplatz als große Symbole anzeigen lassen
	Ansicht → Kleine Symbole	Objekte im Arbeitsplatz als kleine Symbole anzeigen lassen
	Ansicht → Liste	Objekte im Arbeitsplatz in Form einer Liste anzeigen
	Ansicht → Tabelle	Objekte im Arbeitsplatz in Form einer Tabelle anzeigen
	Ansicht → Anpassen	Anzeige der Elemente der Management-Konsole anpassen

Objekt	Menüpunkt	Zweck des Menüpunkts
Kaspersky Security Center	**Erstellen → Administrations-server**	Administrationsserver in Konsolenstruktur einfügen
<Name des Administrationsservers>	**Mit dem Administrations-server verbinden**	Verbindung zum Administrationsserver herstellen
	Vom Administrations-server trennen	Verbindung mit Administrationsserver trennen
Verwaltete Geräte	**Programm installieren**	Assistenten zur Remote-Installation einer Anwendung starten
	Ansicht → Benutzerober-fläche anpassen	Anzeige für die Elemente der Benutzeroberfläche anpassen
	Entfernen	Administrationsserver aus Konsolenstruktur entfernen
	Programm installieren	Assistenten zur Remote-Installation für die Administrations-gruppe starten
	Virenzähler zurücksetzen	Virenzähler für die Geräte der Administrations-gruppe zurücksetzen

Objekt	Menüpunkt	Zweck des Menüpunkts
	Virenaktivität	Bericht über Virenaktivität der Geräte anlegen, die zu einer Administrations-gruppe gehören
	Erstellen → Gruppe	Administrationsgruppe anlegen
	Alle Aufgaben → Gruppenstruktur anlegen	Struktur der Administrations-gruppen anhand der Domänenstruktur oder der Struktur des Active Directory anlegen
	Alle Aufgaben → Nachricht anzeigen	Assistent für das Erstellen einer Benutzermeldung für die Geräte der Administrations-gruppe starten
Verwaltete Geräte → Administrationsserver	**Erstellen → Untergeordneter Administrationsserver**	Assistenten zum Hinzufügen des untergeordneten Administrationsservers starten
	Erstellen → Virtueller Administrationsserver	Assistenten zum Hinzufügen des virtuellen Administrationsservers starten

Objekt	Menüpunkt	Zweck des Menüpunkts
Geräteauswahlen	**Erstellen → Neue Auswahl**	Geräteauswahl erstellen
	Alle Aufgaben → Importieren	Auswahl aus Datei importieren
Programmverwaltung → Programmkategorien	**Kategorie → erstellen**	Programmkategorie erstellen
Programmverwaltung → Programm-Registry	**Filter**	Filter für die Programmliste einstellen
	Zu überwachende Anwendungen	Veröffentlichung der Ereignisse über die Programminstallation einstellen
	Nicht installierte Programme löschen	Informationen über Programme, die nicht mehr auf den Geräten des Netzwerks installiert sind, aus der Liste löschen

Objekt	Menüpunkt	Zweck des Menüpunkts
Programmverwaltung → Software-Updates	**Lizenzverträge für Updates akzeptieren**	Endbenutzer-Lizenzvertrag für Software-Updates akzeptieren
Programmverwaltung → Lizenzen für Software von Kaspersky Lab	**Schlüssel hinzufügen**	Schlüssel zur Datenverwaltung des Administrations-servers hinzufügen
	Programm aktivieren	Assistenten für die Erstellung einer Aufgabe zur Programmaktivierung starten
	Bericht über Schlüssel	Bericht über Schlüssel auf den Client-Geräten erstellen und ansehen
Programmverwaltung → Lizenzverwaltung für Drittanbieter-Software	**Erstellen → Lizenzierte Programmgruppe**	Lizenzierte Programmgruppe erstellen
Mobile Geräte verwalten → Mobile Geräte	**Erstellen → Mobilgerät**	Neues mobiles Gerät des Benutzers verbinden
Mobile Geräte verwalten → Zertifikate	**Erstellen → Zertifikat**	Zertifikat erstellen
	Erstellen → Mobilgerät	Neues mobiles Gerät des Benutzers verbinden

Objekt	Menüpunkt	Zweck des Menüpunkts
Remote-Installation → Installationspakete	**Aktuelle Versionen der Programme anzeigen**	Liste der aktuellen Versionen von Kaspersky-Lab-Programmen ansehen, die auf Kaspersky-Lab-Internetservern zur Verfügung stehen
	Erstellen → Installationspaket	Installationspaket erstellen
	Alle Aufgaben → Datenbanken aktualisieren	Programm-Datenbanken in den Installations-paketen aktualisieren
	Alle Aufgaben → Gemeinsame Liste der autonomen Pakete anzeigen	Gemeinsame Liste der autonomen Installationspakete ansehen, die für Installationspakete erstellt wurden

Objekt	Menüpunkt	Zweck des Menüpunkts
Netzwerkabfrage → Domänen	**Alle Aufgaben → Geräteaktivität**	Einstellungen für die Reaktion des Administrationsservers auf fehlende Aktivität von Geräten im Netzwerk konfigurieren
Netzwerkabfrage → IP-Bereiche	**Erstellen → IP-Bereich**	IP-Bereich erstellen
Datenverwaltung → Updates und Patches für Software von Kaspersky Lab	**Updates laden**	Aufgabe für das Herunterladen von Updates in die Datenverwaltung starten
	Einstellungen für Update-Download	Einstellungen der Aufgabe für das Herunterladen von Updates in die Datenverwaltung des Administrationsservers anpassen
	Bericht über Datenbankversionen	Bericht über Datenbankversionen anlegen und anzeigen
	Alle Aufgaben → Update-Speicher leeren	Update-Datenverwaltung auf dem Administrationsserver leeren
Datenverwaltung → Hardware	**Erstellen → Gerät**	Netzwerkgerät erstellen

Verbindungsmanager

Im Eigenschaftenfenster der Richtlinie des Administrationsagenten, im untergeordneten Abschnitt **Verbindungsmanager** des Abschnitts **Netzwerk** können Sie die Zeitintervalle für die Übermittlung von Daten an den Administrationsserver durch den Administrationsagenten festlegen.

Verbindung bei Bedarf herstellen Bei dieser Variante wird eine Verbindung dann hergestellt, wenn Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

Verbindung in den angegebenen Zeiträumen herstellen Bei dieser Variante wird eine Verbindung des Administrationsagenten mit dem Administrationsserver in den vorgegebenen Zeiträumen hergestellt. Sie können mehrere Zeiträume für die Verbindung hinzufügen.

Benutzerrechte für die Verwaltung von Exchange ActiveSync-Mobilgeräten

Für die Verwaltung der mobilen Geräte, die über das Protokoll Exchange ActiveSync mit dem Microsoft Exchange Server 2010 oder Microsoft Exchange Server 2013 laufen, ist es erforderlich, dass der Benutzer Mitglied einer Rollengruppe ist, für die die folgenden Cmdlets zugelassen sind:

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy.

Für die Verwaltung der mobilen Geräte, die über das Protokoll Exchange ActiveSync mit dem Microsoft Exchange Server 2007 laufen, ist es erforderlich, dass der Benutzer Administratorrechte hat. Falls der Benutzer keine Administratorrechte hat, müssen Cmdlets ausgeführt werden (s. Tabelle unten).

Tabelle 7. Administratorrechte zur Verwaltung von Exchange ActiveSync-Mobilgeräten für Microsoft Exchange Server 2007

Zugriff	Objekt	Cmdlet
Vollständig	Verzweigung "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	`Add-ADPermission -User <Benutzer- oder Gruppenname> -Identity "CN=Mobile Mailbox Policies,CN=<Unternehmensname>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domänenname>" -InheritanceType All -AccessRight GenericAll`
Lesen	Verzweigung "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	`Add-ADPermission -User <Benutzer- oder Gruppenname> -Identity "CN=<Unternehmensname>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domänenname>" -InheritanceType All -AccessRight GenericRead`
Lesen und Schreiben	Eigenschaften von msExchMobileMailboxPolicyLink und msExchOmaAdminWirelessEnable für Active Directory-Objekte	`Add-ADPermission -User <Benutzer- oder Gruppenname> -Identity "DC=<Domänenname>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
Vollständig	Datenverwaltung der ms-Exch-Store-Admin-Postfächer für mailboxstorages	`Get-MailboxDatabase | Add-ADPermission -User <Benutzer- oder Gruppenname> -ExtendedRights ms-Exch-Store-Admin`

Ausführliche Informationen zur Verwendung von Exchange Management Shell finden Sie auf der Website des Technischen Supports für Microsoft Exchange Server (https://technet.microsoft.com/de-de/library/bb123778(v=exchg.150).aspx).

Über den Administrator des virtuellen Servers

Der Administrator des Unternehmensnetzwerks, das durch einen virtuellen Server verwaltet wird, wird Kaspersky Security Center 10 Web Console starten, um Informationen über den Status des Antiviren-Schutzes des Netzwerks unter dem in diesem Fenster vorgegebenen Benutzerkonto anzuzeigen.

Bei Bedarf können Sie mehrere Benutzerkonten für die Administratoren des virtuellen Servers anlegen.

Der Administrator des virtuellen Administrationsservers ist ein interner Benutzer von Kaspersky Security Center. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

Liste der verwalteten Geräte Spaltenwerte

Die nachfolgende Tabelle enthält Namen und Beschreibungen der Spalten der Liste der verwalteten Geräte.

Tabelle 8. Spaltenwerte der Liste der verwalteten Geräte

Spaltenname	Wert
Name	NetBios-Name des Client-Geräts. Die Symbolbeschreibungen für die Gerätenamen finden Sie im Appendix (s. Abschnitt "Statusmeldungen der Geräte, Aufgaben und Richtlinien" auf S. 430).
Betriebssystem-Typ	Betriebssystem-Typ des Client-Geräts.
Windows-Domäne	Name der Windows-Domäne, zu welcher das Client-Gerät gehört.
Der Agent wurde installiert	Ergebnis der Installation des Administrationsagenten auf dem Client-Gerät.
Der Agent läuft	Ergebnis der Funktion des Administrationsagenten.
Echtzeitschutz	Ein Schutzprogramm ist installiert (*Ja*, *Nein*).
Verbindung mit dem Server	Zeitraum seit der letzten Verbindung des Client-Geräts mit dem Administrationsserver.
Letztes Update	Zeitraum seit dem letzten Update des Kaspersky Security Center Administrationsservers.
Status	Aktueller Status des Client-Geräts (*OK, Kritisch, Warnung)*.
Statusbeschreibung	Gründe für den Wechsel des Status des Client-Geräts zu *Kritisch* oder *Warnung.* Der Gerätestatus wechselt aus folgenden Gründen zu *Warnung* oder *Kritisch*:

Spaltenname	Wert
	• Es wurde kein Schutzprogramm installiert • Viele Viren gefunden • Die Stufe des Echtzeitschutzes unterscheidet sich von der, die vom Administrator eingestellt wurde • Die letzte Virensuche liegt lange zurück • Die Datenbanken sind veraltet • Hatte lange keine Verbindung • Es gibt unbearbeitete Objekte • Neustart erforderlich • Es sind inkompatible Anwendungen installiert • Es wurden Schwachstellen in Programmen gefunden • Die letzte Suche nach Windows-Updates liegt lange zurück • Vordefinierter Zustand der Datenverschlüsselung • Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie • Es sind unbearbeitete Vorfälle vorhanden • Die Gültigkeitsdauer der Lizenz läuft bald ab. Der Gerätestatus wechselt aus folgenden Gründen nur zu *Kritisch*: • Die Gültigkeitsdauer der Lizenz ist abgelaufen • Verbindung zum Client-Gerät unterbrochen • Der Schutz ist deaktiviert • Es wurde kein Schutzprogramm gestartet. Die verwalteten Kaspersky-Lab-Programme auf den Client-Geräten können die Liste der Statusbeschreibungen ergänzen. Kaspersky Security Center kann die Beschreibung des Status des Client-Geräts von den verwalteten Kaspersky-Lab-Programmen auf diesem Gerät erhalten. Wenn der Status,

Spaltenname	Wert
	der dem Gerät durch die verwalteten Programme zugewiesen wurde, nicht mit dem von Kaspersky Security Center zugewiesenen Status übereinstimmt, wird in der Verwaltungskonsole der für die Sicherheit des Geräts kritischste Status angezeigt. Wenn z. B. eines der verwalteten Programme dem Gerät den Status *Kritisch*, Kaspersky Security Center jedoch den Status *Warnung* zugewiesen hat, wird in der Verwaltungskonsole für das Gerät der Status *Kritisch* sowie die Beschreibung dieses Status vom verwalteten Programm angezeigt.
Info update	Zeitraum seit der letzten erfolgreichen Synchronisierung des Client-Geräts mit dem Administrationsserver.
Name der DNS-Domäne	Name der DNS-Domäne des Client-Geräts.
DNS-Domäne	Primäres DNS-Suffix.
IP-Adresse	IP-Adresse des Client-Geräts. Es wird empfohlen, eine IPv4-Adresse zu verwenden.
Das letzte Mal im Netzwerk sichtbar	Dauer der Sichtbarkeit des Client-Geräts im Netzwerk.
Untersuchung auf Befehl	Datum und Uhrzeit der letzten Untersuchung des Client-Geräts, die auf Benutzeranfrage von einem Schutzprogramm ausgeführt wurde.
Virenfunde	Anzahl der gefundenen Viren
Echtzeitschutz-Status	Echtzeitschutz-Status(*Wird gestartet, Wird ausgeführt, Wird ausgeführt (maximaler Schutz), Wird ausgeführt (Höchstgeschwindigkeit), Wird ausgeführt (Empfohlen), Wird ausgeführt (mit den benutzerdefinierten Einstellungen), Beendet, Angehalten, Fehler)*.

Spaltenname	Wert
IP-Adresse der Verbindung	IP-Adresse der Verbindung mit dem Kaspersky Security Center Administrationsserver.
Version des Administrationsagenten	Version des Administrationsagenten.
Schutzversion	Version des Schutzprogramms, das auf dem Client-Gerät installiert ist.
Datenbankversion	Version der Antiviren-Datenbanken.
Einschaltzeit	Datum und Uhrzeit des letzten Einschaltens des Client-Geräts.
Neustart	Ein Neustart des Client-Geräts ist erforderlich.
Update-Agent	Name des Geräts, das die Rolle des Update-Agenten für dieses Client-Gerät übernimmt.
Beschreibung	Beschreibung des Client-Geräts, die beim Scannen des Netzwerks abgefragt wurde.
Verschlüsselungsstatus	Verschlüsselungsstatus der Daten des Client-Geräts.
WUA-Status	Status des Windows-Update-Agenten des Client-Geräts. Der Wert "Ja" bezeichnet Client-Geräte, die Updates über Windows Update vom Administrationsserver erhalten. Der Wert "Nein" bezeichnet Client-Geräte, die Updates über Windows Update aus anderen Quellen erhalten.
Bitanzahl des Betriebssystems	Bitanzahl des Betriebssystems des Client-Geräts.
Status des Schutzes vor Spam	Der Schutzstatus von Spam (*Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehler, Unbekannt)*.

Spaltenname	Wert
Status des Schutzes vor Datenverlust	Status des Schutzes vor Datenverlust (*Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehler, Unbekannt)*.
Schutzstatus für Server für die Zusammenarbeit	Status der Inhaltsfilterung (*Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehler, Unbekannt)*.
Status des Antiviren-Schutzes von Mail-Servern	Status des Antiviren-Schutzes von Mail-Servern (*Wird ausgeführt, Wird gestartet, Beendet, Angehalten, Fehler, Unbekannt)*.

Statusmeldungen der Geräte, Aufgaben und Richtlinien

In der unten stehenden Tabelle befindet sich ein Verzeichnis von Zeichen, die in der Konsolenstruktur und im Arbeitsplatz der Verwaltungskonsole neben den Namen der Geräte, Aufgaben und Richtlinien erscheinen. Diese Zeichnen erläutern den Status der Objekte.

Tabelle 9. Statusmeldungen der Geräte, Aufgaben und Richtlinien

Zeichen	Status
	Gerät mit Betriebssystem für Workstations, das im Netzwerk gefunden wurde und nicht zu einer Administrationsgruppe gehört
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und den Status *OK* aufweist
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und den Status *Warnung* aufweist
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und den Status *Kritisch* aufweist
	Gerät mit Betriebssystem für Workstations, das zu einer Administrationsgruppe gehört und dessen Verbindung zum Administrationsserver unterbrochen wurde

	Gerät mit Betriebssystem für Server, das im Netzwerk gefunden wurde und nicht zu einer Administrationsgruppe gehört
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und den Status *OK* aufweist
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und den Status *Warnung* aufweist
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und den Status *Kritisch* aufweist
	Gerät mit Betriebssystem für Server, das zu einer Administrationsgruppe gehört und dessen Verbindung zum Administrationsserver unterbrochen wurde
	Mobile Geräte, die im Netzwerk gefunden wurden und nicht zu einer Administrationsgruppe gehören
	Mobile Geräte, die zu einer Administrationsgruppe gehören und den Status *OK* haben
	Mobile Geräte, die zu einer Administrationsgruppe gehören und den Status *Warnung* haben
	Mobile Geräte, die zu einer Administrationsgruppe gehören und den Status *Kritisch* haben
	Mobile Geräte, die zu einer Administrationsgruppe gehören, deren Verbindung zum Administrationsserver unterbrochen ist
	Aktive Richtlinie
	Inaktive Richtlinie
	Aktive Richtlinie, die von der auf dem Hauptadministrationsserver erstellten Gruppe vererbt wurde

	Eine aktive Richtlinie, die von einer Gruppe einer übergeordneten Hierarchieebene vererbt wurde
	Aufgabe (Gruppenaufgabe, Aufgabe des Administrationsservers oder für bestimmte Geräte) mit dem Zustand *Wartet auf Ausführung* oder *Abgeschlossen*
	Aufgabe (Gruppenaufgabe, Aufgabe des Administrationsservers oder für bestimmte Geräte) mit dem Zustand *Wird ausgeführt*
	Aufgabe (Gruppenaufgabe, Aufgabe des Administrationsservers oder für bestimmte Geräte) mit dem Zustand *Beendet mit Fehler*
	Aufgabe, die von der auf dem Hauptadministrationsserver erstellten Gruppe vererbt wurde
	Eine Aufgabe, die von einer übergeordneten Hierarchieebene vererbt wurde

Symbole der Status der Dateien in der Verwaltungskonsole

Für die Vereinfachung der Arbeit mit den Dateien in der Verwaltungskonsole von Kaspersky Security Center werden neben den Namen der Dateien Symbole angezeigt. Die Symbole geben Auskunft über den Status, der der jeweiligen Datei von den verwalteten Kaspersky-Lab-Programmen auf den Client-Geräten zugewiesen wird. Die Symbole werden im Arbeitsplatz der Ordner **Quarantäne**, **Backup** und **Dateien mit verschobener Verarbeitung** angezeigt.

Tabelle 10. Übereinstimmung der Symbole mit den Status der Dateien

Zeichen	Status
	Datei mit dem Status *Infiziert*
	Datei mit dem Status *Warnung* oder *Möglicherweise infiziert*
	Datei mit dem Status *Vom Benutzer in den Ordner verschoben*
	Datei mit dem Status *Fehlalarm*
	Datei mit dem Status *Desinfiziert*
	Datei mit dem Status *Gelöscht*
	Datei im Ordner **Quarantäne** mit dem Status *Nicht infiziert, Mit Kennwort geschützt* oder *Muss an Kaspersky Lab gesendet werden*. Wenn neben dem Symbol keine Beschreibung des Status angezeigt wird, dann hat das verwaltete Kaspersky-Lab-Programm auf dem Client-Gerät einen unbekannten Status an Kaspersky Security Center übermittelt.
	Datei im Ordner **Backup** mit dem Status *Virusfrei*, *Mit Kennwort geschützt* oder *Muss an Kaspersky Lab gesendet werden*. Wenn neben dem Symbol keine Beschreibung des Status angezeigt wird, dann hat das verwaltete Kaspersky-Lab-Programm auf dem Client-Gerät einen unbekannten Status an Kaspersky Security Center übermittelt.
	Datei im Ordner **Dateien mit verschobener Verarbeitung** mit dem Status *Virusfrei*, *Mit Kennwort geschützt* oder *Muss an Kaspersky Lab gesendet werden*. Wenn neben dem Symbol keine Beschreibung des Status angezeigt wird, dann hat das verwaltete Kaspersky-Lab-Programm auf dem Client-Gerät einen unbekannten Status an Kaspersky Security Center übermittelt.

Reguläre Ausdrücke in der Suchzeile verwenden

Zur Suche nach einzelnen Wörtern oder Symbolen können Sie die folgenden regulären Ausdrücke in der Suchzeile verwenden:

- *. Ersetzt eine Folge einer beliebigen Anzahl von Zeichen. Zur Suche nach den Wörtern "Server", oder "Server-" geben Sie beispielsweise in der Suchzeile den Ausdruck `Server*` ein.

- ?. Dieses Zeichen ersetzt ein beliebiges Symbol. Zur Suche nach den Wörtern "Fenstern" oder "Fensters" geben Sie beispielsweise den Ausdruck `Fenster?` in der Suchzeile ein.

  > Der Text in der Suchzeile darf nicht mit dem Symbol ? anfangen.

- [<Intervall>]. Ersetzt ein Zeichen aus dem festgelegten Bereich bzw. der festgelegten Menge. Zur Suche nach einer beliebigen Ziffer geben Sie beispielsweise den Ausdruck `[0-9]` in der Suchzeile ein. Zur Suche nach einem der folgenden Symbole a, b, c, d, e, f geben Sie den Ausdruck `[abcdef]` in der Suchzeile ein.

Zur Volltextsuche können Sie die folgenden regulären Ausdrücke in der Suchzeile verwenden:

- Leerzeichen: Dieses Zeichen bedeutet, dass im Text mindestens eines der Wörter vorhanden sein muss, die durch ein Leerzeichen getrennt in der Suchzeile eingegeben wurden. Zur Suche nach einer Phrase, die das Wort "Untergeordnet" oder "Virtuell" (bzw. beide Wörter) enthält, geben Sie beispielsweise den Ausdruck `Untergeordnet Virtuell` in der Suchzeile ein.

- Zeichen "plus" (+), AND oder &&. Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss. Zur Suche nach einer Phrase, die das Wort "Untergeordnet" und das Wort "Virtuell" enthält, können Sie beispielsweise die folgenden Ausdrücke in der Suchzeile eingeben: `+Untergeordnet+Virtuell`, `Untergeordnet AND Virtuell`, `Untergeordnet && Virtuell`.

- OR oder ||. Zwischen den Wörtern stehend bedeutet dieses Zeichen, dass eines der Wörter im Text vorhanden sein muss. Zur Suche nach einer Phrase, die das Wort "Untergeordnet" oder das Wort "Virtuell enthält", können Sie beispielsweise die folgenden Ausdrücke

in der Suchzeile eingeben: `Untergeordnet OR Virtuell`, `Untergeordnet || Virtuell`.

- Zeichen "minus" (-). Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf. Zur Suche nach einer Phrase, in der das Wort "Untergeordnet" vorhanden sein und das Wort "Virtuell" fehlen muss, geben Sie beispielsweise den Ausdruck `+Untergeordnet-Virtuell` in der Suchzeile ein.

- `"<Textabschnitt>"`: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein. Zur Suche nach einer Phrase, die den Ausdruck "Untergeordneter Server" enthält, geben Sie beispielsweise den Ausdruck `"Untergeordneter Server"` in der Suchzeile ein.

Die Volltextsuche ist in den folgenden Filterblöcken verfügbar:

- Filterblock der Ereignisliste nach Spalten **Ereignis** und **Beschreibung**

- Filterblock für Benutzerkonten nach Spalte **Name**

- Filterblock der Programm-Registry nach Spalte **Name**, wenn das Kontrollkästchen **Programme nach Namen gruppieren** deaktiviert ist.

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.

Administrative Rechte

Berechtigungen eines Benutzers zur Verwaltung von Exchange-Objekten innerhalb einer Exchange-Organisation.

Aktiver Schlüssel

Schlüssel, der im Augenblick für die Programmausführung verwendet wird.

Allgemeines Zertifikat

Zertifikat zur Identifikation des mobilen Geräts des Benutzers.

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.

App-Store

Programmkomponente von Kaspersky Security Center. Der App Store wird für die Installation von Apps auf die Android-Geräte der Benutzer verwendet. Im App Store können apk-Dateien der Apps und Links zu den Apps in Google Play veröffentlicht werden.

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.

Authentifizierungsagent

Benutzeroberfläche, die eine Authentifizierung ermöglicht, um Zugriff auf verschlüsselte Festplatten zu erhalten und das Betriebssystem nach der Verschlüsselung der Systemfestplatte herunterzuladen.

B

Broadcast-Domäne

Logischer Abschnitt eines Computernetzwerks, in dem alle Knoten über einen Breitbandkanal auf der Ebene des OIS-Netzwerkmodells (Open Systems Interconnection Basic Reference Model) untereinander Daten austauschen können.

C

Client des Administrationsservers (Client-Gerät)

Gerät (Server oder Arbeitsstation), auf dem der Administrationsagent und die zu verwaltenden Kaspersky-Lab-Programme installiert sind.

D

Demilitarisierte Zone (DMZ)

Bei der demilitarisierten Zone handelt es sich um ein Segment des lokalen Netzwerks, in dem sich die Server befinden, die auf Anfragen aus dem globalen Netzwerk reagieren. Zur Gewährleistung der Sicherheit des lokalen Netzwerks des Unternehmens ist der Zugriff auf das lokale Netzwerk von der demilitarisierten Zone aus eingeschränkt und durch eine Firewall geschützt.

E

EAS-Gerät

Ein mobiles Gerät, das mit dem Administrationsserver mit dem Exchange ActiveSync-Protokoll verbunden wird. Über das Exchange ActiveSync-Protokoll können Geräte mit den Betriebssystemen iOS, Android und Windows Phone® angeschlossen und verwaltet werden.

Ereigniskategorie des Patches

Charakteristik des Patches. Für Patches von Drittanbietern oder von Microsoft existieren fünf Ereigniskategorien:

- Kritisch
- Hoch
- Normal.
- Niedrig
- Unbekannt.

Die Ereigniskategorie des Drittanbieter- oder Microsoft-Patches wird bestimmt durch die kritischste Signifikanz der Schwachstelle, die der Patch schließt.

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

Geräteinhaber

Der Geräteinhaber ist jener Benutzer des Geräts, an den sich der Administrator wenden kann, wenn bestimmte Arbeiten am Gerät durchgeführt werden müssen.

Gruppenaufgabe

Aufgabe für eine Administrationsgruppe. Wird auf allen Client-Geräten ausgeführt, die zu dieser Administrationsgruppe gehören.

H

Heim-Administrationsserver

Der Heim-Administrationsserver ist ein Administrationsserver, der bei der Installation des Administrationsagenten angegeben wurde. Der Heim-Administrationsserver kann in den Einstellungen der Verbindungsprofile des Administrationsagenten verwendet werden.

I

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.

Interne Benutzer

Die Benutzerkonten der internen Benutzer werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Unter dem Benutzerkonto eines internen Benutzers kann der Administrator eines virtuellen Servers die Kaspersky Security Center 10 Web Console starten, um sich Informationen über den Status der Antiviren-Sicherheit des Netzwerks anzeigen zu lassen. Innerhalb der Funktionen von Kaspersky Security Center verfügen die internen Benutzer über die Berechtigungen tatsächlicher Benutzer.

Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center erstellt und verwendet. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center.

iOS MDM-Gerät

Ein mobiles Gerät, das über das iOS MDM-Protokoll an den iOS MDM-Server angeschlossen wird. Über das iOS MDM-Protokoll können Geräte mit dem Betriebssystem iOS angeschlossen und verwaltet werden.

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 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 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.

Kaspersky Security Network (KSN)

Infrastruktur der Cloud-Dienste, die den umfassenden Zugriff zur Kaspersky-Lab-Wissensdatenbank über die Reputation von Dateien, Web-Ressourcen und Software gewährleistet. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Lab-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

KES-Gerät

Ein mobiles Gerät, das mit dem Administrationsserver verbunden ist und mithilfe der mobilen App Kaspersky Security für Android verwaltet wird.

Konfigurationsprofil

Richtlinie, die Einstellungen und Einschränkungen für ein mobiles iOS MDM-Gerät umfasst.

L

Lizenzierte Programmgruppe

Gruppe von Programmen, die anhand der vom Administrator festgelegten Kriterien erstellt wurde (z. B. nach dem Hersteller), für welche die Anzahl von Installationen auf den Client-Geräten registriert wird.

Lokale Aufgabe

Aufgabe, die für ein einzelnes Client-Gerät festgelegt wurde und darauf ausgeführt werden soll.

M

MDM-Richtlinie

Eine Auswahl von Programmeinstellungen, die für die Verwaltung von mobilen Geräten über Kaspersky Security Center angewendet werden. Zur Verwaltung verschiedener Typen von mobilen Geräten werden verschiedene Programmeinstellungen verwendet. Die Richtlinie umfasst Einstellungen zur vollständigen Konfiguration der gesamten Anwendungsfunktionalität.

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

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 Computern 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 Computern jeder Administrationsgruppe installiert sind. Im Rahmen einer Administrationsgruppe kann jedoch für jedes Programm immer nur eine Richtlinie gleichzeitig angewendet werden.

Rollengruppe

Eine Gruppe von Benutzern von Exchange ActiveSync-Mobilgeräten, die die gleichen administrativen Rechte haben (s. Abschnitt "Administrative Rechte" auf S. 436).

S

Schwachstelle

Ein Fehler in einem Betriebssystem bzw. in einem Programm, der von Malware-Herstellern ausgenutzt werden kann, um in das Betriebssystem bzw. das Programm einzudringen und seine Integrität zu beschädigen. Eine große Menge von Schwachstellen macht das Betriebssystem anfällig, da die ins Betriebssystem eingedrungenen Viren Störungen des Systems und der installierten Programme verursachen können.

Server für mobile Geräte

Eine Komponente von Kaspersky Security Center, die den Zugriff auf mobile Geräte bereitstellt und deren Verwaltung über die Verwaltungskonsole ermöglicht.

Subnet Network Location Awareness

Network Location Awareness Subnetz (NLA-Subnet); dieses Subnetz besteht aus einer manuell erstellten Auswahl an Geräten. Im Rahmen des Funktionsumfangs von Kaspersky Security Center kann ein NLA-Subnet verwendet werden, um eine manuelle Auswahl von Geräten, auf die der Update-Agent Updates verteilen soll, zu erstellen.

U

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.

Virenangriff

Der Versuch, ein Gerät mit einem Virus oder anderer Schadsoftware zu infizieren.

Virtueller Administrationsserver

Eine Komponente von Kaspersky Security Center, die dazu konzipiert ist, das Schutzsystem im Netzwerk eines Kundenunternehmens zu verwalten.

Ein virtueller Administrationsserver stellt einen besonderen Fall eines untergeordneten Administrationsservers dar und weist im Vergleich zu einem physikalischen Administrationsserver folgende Einschränkungen auf:

- Ein virtueller Administrationsserver kann nur dann funktionieren, wenn er zum Hauptadministrationsserver gehört.
- Ein virtueller Administrationsserver verwendet die Datenbank des Hauptadministrationsservers: Aufgaben zum Erstellen von Sicherungskopien und zur Datenwiederherstellung, Aufgaben zur Update-Überprüfung und Aufgaben zum Download von Updates werden auf dem virtuellen Server nicht unterstützt. Diese Aufgaben werden auf dem Hauptadministrationsserver ausgeführt.
- Für virtuelle Server können keine untergeordneten Administrationsserver angelegt werden (einschl. virtueller Server).

W

Windows Server Update Services (WSUS)

Programm, das zur Verteilung von Updates für Microsoft-Programme auf den Benutzercomputern eines Unternehmensnetzwerks verwendet wird.

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.

Wiederherstellung

Die Wiederherstellung entspricht dem Verschieben des ursprünglichen Objektes aus der Quarantäne oder aus dem Backup in den Ausgangsordner, in dem das Objekt bis zu dessen Verschiebung in die Quarantäne, dessen Desinfizierung oder Löschung gespeichert wurde, oder in einen anderen Ordner, den der Benutzer angegeben hat.

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 38 Büros in 33 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

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.

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.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Active Directory, ActiveSync, Excel, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SQL Server, Tahoma, Windows, Windows Server, Windows Phone und Windows Vista sind eingetragene Marken der Microsoft Corporation in den USA und anderen Ländern.

Adobe ist in den Vereinigten Staaten von Amerika und/oder in anderen Ländern ein Warenzeichen bzw. eine eingetragene Marke von Adobe Systems Incorporated.

AirPlay, AirDrop, AirPrint, App Store, Apple, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger sind in den USA und in anderen Ländern eingetragene Marken von Apple Inc.

AMD, AMD64 sind eingetragene Marken von Micro Devices, Inc.

Apache und Apache feather logo sind Markenzeichen von Apache Software Foundation.

BlackBerry ist eine eingetragene Marke der Research In Motion Limited in den USA. Die Marke kann auch in anderen Ländern angemeldet werden.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Cisco, Cisco Systems, IOS sind eingetragene Marken von Cisco Systems, Inc. und/oder ihren Tochtergesellschaften in den USA und in 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.

Android, Chrome, Google, Google Play, Google Maps und Youtube sind Markenzeichen von Google, 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.

QRadar ist ein Markenzeichen der International Business Machines Corporation, und ist in vielen Ländern der Welt eingetragen.

CentOS, Fedora und Red Hat Enterprise Linux sind in den USA und in anderen Ländern eingetragene Marken von Red Hat Inc.

Linux ist ein eingetragenes Markenzeichen von Linus Torvalds in den USA und anderen Ländern.

Novell ist ein eingetragenes Markenzeichen von Novell Inc. in den USA und anderen Ländern.

Das Markenzeichen Symbian ist Eigentum der Symbian Foundation Ltd.

SPL, Splunk sind in den USA und anderen Ländern eingetragene Marken von Splunk, Inc.

SUSE ist eine in den USA und in anderen Ländern eingetragene Marke von SUSE LLC.

UNIX ist ein in den USA und anderen Ländern eingetragenes Markenzeichen. Die Nutzung ist durch die X/Open Company Limited lizenziert.

VMware, VMware vSphere sind Marken von VMware, Inc. oder in den USA oder in anderen Ländern eingetragene Marken von VMware, Inc.

Sachregister

A

B

C

D

E

G

H

I

K

L

M

N

P

R

S

U

V

Z