KASPERSKY lab

Kaspersky Security Center 10

Implementation Guide

Application version: 10 Service Pack 2, Maintenance Release 1

Dear User,

Thank you for your trust! We hope that this document will help you in your work and will provide answers regarding this software product.

Warning! This document is the property of Kaspersky Lab: All rights to this document are protected by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may only be used for informational, non-commercial, and personal purposes.

This document may be amended without additional notification.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 12/7/2016

© 2017 AO Kaspersky Lab. All Rights Reserved.

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

Table of Contents

About this document 8
In this document 8
Document conventions 11
Sources of information about the application 13
Sources for unassisted search of information 13
Discussing Kaspersky Lab applications on the forum 15
Kaspersky Security Center 16
Application architecture 18
Hardware and software requirements 19
Information about Administration Server performance 35
Selecting a structure of an organization protection system 37
Typical schemes of protection system deployment 40
Deploying a protection system within an organization 41
Deploying a protection system via Administration Console within an organization 41
Deploying a protection system using Kaspersky Security Center 10 Web Console within an organization 42
Deploying a protection system manually within an organization 43
Deploying a protection system on a client organization's network 45
Deploying a protection system using Administration Console on a client organization's network 45
Deploying a protection system using Kaspersky Security Center 10 Web Console on a client's corporate network 46
Deploying a protection system on a client organization's network manually 47
Deploying Administration Server 49
Stages of deploying Administration Server within an enterprise 50
Steps of Administration Server deployment for protection of a client organization's network 50
Upgrading Kaspersky Security Center 50
Installing and removing Kaspersky Security Center 52
Preparing for installation 53

Standard installation 56
Custom installation 57
Installation in non-interactive mode 67
Changes in the system after installing the application 74
Removing the application 77
Installing Administration Console on the administrator's workstation 78
Configuring the connection of Administration Console to Administration Server 79
Installing and configuring Kaspersky Security Center SHV 80
Installing Kaspersky Security Center 10 Web Console 82
Step 1. Reviewing the License Agreement 83
Step 2. Connecting to Kaspersky Security Center 84
Step 3. Selecting the destination folder 85
Step 4. Selecting the Apache server installation mode 85
Step 5. Installing Apache Server 85
Step 6. Selecting the ports 86
Step 7. Selecting an account 86
Step 8. Starting Kaspersky Security Center 10 Web Console installation 86
Step 9. Completing Kaspersky Security Center 10 Web Console installation 87
Upgrading Kaspersky Security Center 10 Web Console 87
Advanced configuration of Kaspersky Security Center 10 Web Console and Self Service Portal 88
Changing the port number for device connection 88
Configuring a License Agreement file and an FAQ file 90
Configuring a logo 90
Configuring a protection system for a client organization's network 91
Assigning a device to act as update agent. Configuring an update agent 92
Local installation of Network Agent on a device selected to act as update agent 93
Prerequisites for installing applications on devices of a client organization 95
Creating a hierarchy of administration groups subordinate to the virtual Administration Server 96
Remote installation of applications 97
Installing applications using a remote installation task 100
Installing an application on selected devices 101
Installing an application on client devices in an administration group 102

Installing an application using Active Directory group policies 103
Installing applications on slave Administration Servers 105
Installing applications using Remote Installation Wizard 106
Viewing a protection deployment report..... 107
Remote removal of applications 109
Remote removal of an application from client devices of an administration group110
Remote removal of an application from selected devices 110
Work with installation packages 111
Creating an installation package..... 112
Distributing installation packages to slave Administration Servers 113
Distributing installation packages through update agents 114
Transferring application installation results to Kaspersky Security Center 114
Retrieving up-to-date versions of applications..... 116
Preparing a device for remote installation. Utility tool riprep.exe 118
Preparing a device for remote installation in interactive mode 120
Preparing a device for remote installation in non-interactive mode..... 121
Local installation of applications 123
Local installation of Network Agent 125
Installing Network Agent in non-interactive mode 127
Local installation of the application management plug-in..... 129
Installing applications in non-interactive mode 130
Installing software by using stand-alone packages 131
Deploying mobile device management systems..... 132
Management through iOS MDM and Microsoft Exchange ActiveSync 132
Installing a Mobile device server for Exchange ActiveSync 134
Connecting mobile devices to a Microsoft Exchange Mobile Devices Server 135
Deploying a system for management via iOS MDM protocol 136
Installing iOS MDM Server..... 138
Installing iOS MDM Server in non-interactive mode 140
Use of iOS MDM Server by multiple virtual Servers 142
Receiving an APNs certificate..... 143
Installing an APNs certificate on an iOS MDM Server 145
Issuing and installing a shared certificate on a mobile device..... 146
Adding an iOS MDM device to the list of managed devices..... 146

Deploying a system for management via KES protocol using Self Service Portal ... 148
Adding a KES device to the list of managed devices ... 149
Installing Self Service Portal ... 151
Step 1. Reviewing the License Agreement ... 152
Step 2. Connecting to Kaspersky Security Center ... 152
Step 3. Selecting the destination folder ... 153
Step 4. Selecting the Apache server installation mode ... 154
Step 5. Installing Apache Server ... 154
Step 6. Selecting the ports ... 155
Step 7. Selecting an account ... 156
Step 8. Running installation of Self Service Portal ... 156
Step 9. Finishing installation of Self Service Portal ... 156
Configuring SMS delivery in Kaspersky Security Center ... 157
Retrieving and installing Kaspersky SMS Broadcasting utility ... 158
Synchronization of a mobile device with Administration Server ... 159
Assigning a mobile device as the SMS sender ... 160
Network load ... 161
Initial deployment of anti-virus protection ... 162
Initial update of anti-virus databases ... 163
Synchronizing a client with the Administration Server ... 163
Additional update of anti-virus databases ... 165
Processing of events from clients by Administration Server ... 166
Traffic per 24 hours ... 167
Rate of adding Kaspersky Endpoint Security events to the database ... 168
Contacting the Technical Support Service ... 169
How to obtain technical support ... 169
Technical support by phone ... 170
Technical Support via Kaspersky CompanyAccount ... 170

Glossary 172
AO Kaspersky Lab 183
Enhanced protection with Kaspersky Security Network 185
Information about third-party code 186
Trademark notices 187
Index 189

About this document

Kaspersky Security Center 10 ("Kaspersky Security Center") Implementation Guide is intended for professionals who install and administer Kaspersky Security Center, as well as for those who provide technical support to organizations that use Kaspersky Security Center.

You can use this Guide to:

- Plan the application installation (taking into account the application operation principles, system requirements, standard deployment schemes, and features of compatibility with other applications).
- Prepare Kaspersky Security Center for installation, installing and activating the application.
- Configure the application after installation.

This Guide also lists sources of information about the application and ways to get technical support.

In this section:

In this document 8

Document conventions 11

In this document

The Kaspersky Security Center Implementation Guide contains an introduction, sections describing installation of application components and their interaction configuration, sections that describe deploying of anti-virus protection on a network, sections containing stress testing results, and a glossary.

Sources of information about the application (see page 13)

This section lists the sources of information about the application.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

Kaspersky Security Center (see page 16)

The section contains information on the purpose of Kaspersky Security Center, and its main features and components.

Application architecture (see page 18)

This section describes the Kaspersky Security Center components and their interaction.

Hardware and software requirements (see page 19)

This section describes the hardware and software requirements for networked client devices.

Administration Server performance details (see page 35)

This section represents data on the performance of Administration Server for different hardware configurations.

Standard deployment schemes of anti-virus protection (see page 40)

This section describes standard deployment schemes of a protection system on an enterprise network using Kaspersky Security Center.

Deploying a protection system within an organization (see page 41)

This section describes processes of protection system deployment within an enterprise that correspond to the standard deployment schemes.

Deploying a protection system on a client organization's network (see page 45)

This section describes processes of protection system deployment on a client organization's network that correspond to the standard deployment schemes.

Deploying Administration Server (see page 49)

This section describes stages of Administration Server deployment.

Configuring a protection system in a client organization's network (see page 91)

This section describes the specifics of configuring a protection system using Administration Console in a client organization's network.

Remote installation of applications (see page 97)

This section describes the methods for remote installation of Kaspersky Lab applications and their removal from networked devices.

Local installation of applications (see page 123)

This section provides the installation procedure for applications that can only be installed on a local device.

Deploying mobile device management systems (see page 132)

This section describes the deployment of mobile device management systems via Exchange ActiveSync®, iOS MDM, and Kaspersky Endpoint Security protocols.

Deploying Self Service Portal (see page 150)

This section describes the preparation for deployment of Self Service Portal and the steps of Self Service Portal deployment.

Configuring SMS delivery in Kaspersky Security Center (see page 157)

This section describes installation of Kaspersky SMS Broadcasting utility to a mobile device, synchronization of the utility with Administration Server, and configuration of SMS delivery in Administration Console.

Network load (see page 161)

This section contains information about the volume of network traffic exchanged between client devices and the Administration Server during key administrative operations.

Speed rate for filling up the Administration Server database with events (see page 168)

This section contains examples showing various speed rates for filling up the Administration Server database with events that occur in the operation of managed applications.

Contacting the Technical Support Service (see page 169)

This section provides information about the ways and conditions for providing you technical support.

Glossary

This section lists terms used in the guide.

AO Kaspersky Lab (see page 183)

This section provides information about Kaspersky Lab.

Information about third-party code (see page 186)

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.

Trademark notices (see page 187)

This section contains registered trademark notices.

Index

This section helps you find necessary data quickly.

Document conventions

Document conventions are used herein (see the table below).

Table 1. Document conventions

Sample text	Document conventions description
Note that...	Warnings are highlighted in red and boxed. Warnings contain information about actions that may lead to some unwanted outcome.
We recommend that you use...	Notes are boxed. Notes contain additional and reference information.

Sample text	Document conventions description
Example: …	Examples are on a blue background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following elements are italicized in the text: • New terms • Names of application statuses and events
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are all uppercase. Names of keys that are connected by a plus sign (+) sign indicate the use of a key combination. These keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as entry fields, menu items, and buttons, appear in bold.
► *To configure task schedule:*	Introductory phrases of procedures are italicized and accompanied by the arrow sign.
Enter `help` in the command line The following message then appears: `Specify the date in MM:DD:YY format.`	The following types of text content are set off with a special font: • Text in the command line • Text of messages displayed on the screen by the application • Data that the user has to enter from the keyboard
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be inserted, with angle brackets omitted.

Sources of information about the application

This section lists the sources of information about the application.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

In this section:

Sources for unassisted search of information 13

Discussing Kaspersky Lab applications on the forum..... 15

Sources for unassisted search of information

You can use the following sources to find information about Kaspersky Security Center:

- Kaspersky Security Center page on the Kaspersky Lab website.
- Kaspersky Security Center page on the Technical Support Service website.
- Online help.
- Documentation.

If you cannot find a solution for your issue, we recommend that you contact the Kaspersky Lab Technical Support Service (see section "Contacting the Technical Support Service" on page 169).

An Internet connection is required to use online information sources.

Kaspersky Security Center page on the Kaspersky Lab website

On the Kaspersky Security Center page (http://www.kaspersky.com/security-center), you can view general information about the application, its functions and features.

The Kaspersky Security Center page contains a link to eStore. There you can purchase or renew the application.

Page of Kaspersky Security Center in the Knowledge Base

Knowledge Base is a section on the Technical Support Service website.

On the Kaspersky Security Center page (http://support.kaspersky.com/ksc10), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only to Kaspersky Security Center but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

Online help

The application includes full help files and context help files.

Full help provides information about how to configure and use Kaspersky Security Center.

Use the context help to find information about windows of Kaspersky Security Center, i.e., the descriptions of various settings of Kaspersky Security Center and the links to the descriptions of tasks that use those settings.

Help can be included in the application or published online on the Kaspersky Lab web resource. If Help is published online, the browser window opens when you call it. An Internet connection is required to view online Help.

Documentation

Application documentation consists of the files of application guides.

The administrator's guide provides information on how to configure and use Kaspersky Security Center.

The implementation guide provides instructions on:

- Plan the application installation (taking into account the application operation principles, system requirements, standard deployment schemes, and features of compatibility with other applications).
- Prepare Kaspersky Security Center for installation, installing and activating the application.
- Configure the application after installation.

The Getting Started guide provides information needed to start using the application quickly (a description of the interface and main tasks that can be performed using Kaspersky Security Center).

Discussing Kaspersky Lab applications on the forum

If your question does not require an immediate answer, you can discuss it with the Kaspersky Lab experts and other users in our forum (http://forum.kaspersky.com).

In this forum you can view existing topics, leave your comments, create new topics.

Kaspersky Security Center

The section contains information on the purpose of Kaspersky Security Center, and its main features and components.

Kaspersky Security Center is designed for centralized execution of basic administration and maintenance tasks in an organization's network. The application provides the administrator with access to detailed information about the organization's network security level; it lets you configure all the components of protection based on Kaspersky Lab applications.

Kaspersky Security Center is an application aimed at corporate network administrators and employees responsible for protection of devices in various organizations.

Using Kaspersky Security Center, you can:

- Create a hierarchy of Administration Servers to manage the organization's network, as well as networks at remote offices or client organizations.

  The *client organization* is an organization, whose anti-virus protection is ensured by service provider.

- Create a hierarchy of administration groups to manage a selection of client devices as a whole.

- Manage an anti-virus protection system built based on Kaspersky Lab applications.

- Create images of operating systems and deploy them on client devices over the network, as well as performing remote installation of applications by Kaspersky Lab and other software vendors.

- Remotely manage applications by Kaspersky Lab and other software vendors installed on client devices: install updates, find and fix vulnerabilities.

- Perform centralized deployment of keys for Kaspersky Lab applications to client devices, monitor their use, and renew licenses.

- Receive statistics and reports about the operation of applications and devices.
- Receive notifications about critical events in the operation of Kaspersky Lab applications.
- Manage mobile devices that support Kaspersky Security for Android™, Exchange ActiveSync®, or iOS Mobile Device Management (iOS MDM) protocols.
- Manage encryption of information stored on the hard drives of devices and removable drives and users' access to encrypted data.
- Perform inventory of hardware connected to the organization's network.
- Centrally manage files moved to Quarantine or Backup by security applications, as well as manage files for which processing by security applications has been postponed.

Application architecture

This section describes the Kaspersky Security Center components and their interaction.

Kaspersky Security Center comprises the following main components:

- **Administration Server** (hereinafter also referred to as the *Server*). Centralizes storage of information about applications installed on the organization's network and about how to manage them.
- **Network Agent** (hereinafter also referred to as *Agent*). Coordinates the interaction between Administration Server and Kaspersky Lab applications installed on a network node (workstation or server). This component is common for all of the company's applications for Microsoft® Windows®. Separate versions of Network Agent exist for Kaspersky Laboratory products developed for Novell® and Unix™ systems.
- **Administration Console** (hereinafter also referred to as the *Console*). Provides a user interface to the administration services of the Administration Server and Network Agent. Administration Console is implemented as a snap-in for Microsoft Management Console (MMC). Administration Console allows remote connection to Administration Server over the Internet.
- **Mobile device server**. Provides access to mobile devices and allows managing them through Administration Console. The Mobile device server retrieves information about mobile devices and stores their profiles.
- **Kaspersky Security Center 10 Web Console**. Designed to monitor the status of the protection system of a client organization's network managed by Kaspersky Security Center.

Hardware and software requirements

Administration Server

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 4 GB.
- Available disk space: 10 GB. When using Systems Management, at least 100 GB free disk space shall be available.

Software requirements:

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

Operating system:

- 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.
- Microsoft 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 Edition 64-bit.
- Windows Server 2016 Standard Edition 64-bit.

Database server (can be installed on a different computer):

- 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 (all editions) 32-bit / 64-bit.
- Microsoft SQL Server 2008 R2 (all editions) 64-bit.
- Microsoft SQL Server 2008 R2 Service Pack 2 64-bit.
- Microsoft SQL Server 2012 (all editions) 64-bit.
- Microsoft SQL Server 2014 (all editions) 64-bit.
- Microsoft SQL Server 2016 (all editions) 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.

The following virtual platforms are supported:

- 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 (Windows guest operating systems are supported).

Kaspersky Security Center 10 Web Console

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- For Microsoft Windows operating systems with Kaspersky Security Center Administration Server 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.
- Microsoft 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 Edition 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 (up to 6.6) 64-bit.

Kaspersky Security Center 10 Web Console does not support versions of operating systems that are compatible with systemd, such as Fedora® 17.

Web server:

- Apache 2.4.25 (for Windows) 32-bit.
- Apache 2.4.25 (for Linux) 32-bit / 64-bit.

You can use the following browsers for working with Kaspersky Security Center 10 Web Console:

- Microsoft Internet Explorer® 9 and later.
- Microsoft® Edge™.
- Chrome™ 53 and later.
- Firefox™ 47 and later.
- Safari® 8 under Mac OS X 10.10 (Yosemite).
- Safari 9 under Mac OS X 10.11 (El Capitan).

iOS Mobile Device Management (iOS MDM) mobile device server

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 2 GB.
- Available disk space: 2 GB.

Software requirements: Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server).

Microsoft Exchange Mobile Devices Server

All software and hardware requirements for Microsoft Exchange Mobile Devices Server are included in the requirements for the Microsoft Exchange Server.

Working with Microsoft Exchange Server 2007, Microsoft Exchange Server 2010, and Microsoft Exchange Server 2013 is supported.

Administration Console

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server).
- Microsoft Management Console 2.0.
- Microsoft Windows Installer 4.5.
- Microsoft Internet Explorer 7.0 or later when working with Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, or Microsoft Windows Vista®.
- Microsoft Internet Explorer 8.0 or later when using Microsoft Windows 7.
- Microsoft Internet Explorer 10.0 or later when using Microsoft Windows 8 and 10.
- Microsoft Edge when using Microsoft Windows 10.

Network Agent

Hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

If the device with Network Agent installed also acts as update agent, this device must meet the following hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 1 GB.
- Available disk space: 4 GB.

Software requirements:

- 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 Foundation 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 (up to 7.8) 32-bit.
- Debian GNU / Linux 7.x (up to 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 (up to 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.

You can obtain information about the latest version of the hardware and software requirements from the Technical Support Service website on the application page of Kaspersky Security Center in the System requirements section (http://support.kaspersky.com/ksc10#requirements).

Information about Administration Server performance

This section represents data on the performance of Administration Server for different hardware configurations.

Results of Administration Server performance testing allowed us to define the maximum numbers of client devices with which Administration Server can be synchronized within specified time periods. This information can be used to identify the optimal scheme for deploying anti-virus protection on corporate networks.

The following hardware configurations of the Administration Server were used for testing:

- 32-bit operating system (dual-core Intel® Core™2 Duo E8400 with a clock rate of 3.00 GHz, 4 GB RAM, and SATA 500 GB hard drive).
- 64-bit operating system (4-core processor Intel Xeon® E5450 with a clock rate of 3.00 GHz, 8 GB RAM, and SAS 2x320 RAID 0 hard drive).

The Microsoft SQL Server 2005x32 Enterprise Edition database server was installed on the same client device as Administration Server.

Administration Server of both hardware configurations supported creation of 200 virtual Administration Servers.

Table 2. Summarized results of Administration Server performance testing under a 32-bit operating system

Synchronization interval (min)	Number of managed devices
15	5,000
30	10,000
45	15,000
60	20,000

Table 3. Summarized results of Administration Server performance testing under a 64-bit operating system

Synchronization interval (min)	Number of managed devices
15	10,000
30	20,000
45	30,000
60	40,000

If you connect Administration Server to a MySQL or SQL Express database server, we recommend that you avoid to use the application to manage more than 5,000 devices.

Selecting a structure of an organization protection system

Selection of a structure for an organization protection system is defined by the following factors:

- Organization's network topology.
- Organizational structure.
- Number of employees in charge of the network protection, and allocation of their responsibilities.
- Hardware resources that can be allocated in order to install protection management components.
- Throughput of communication channels that can be allocated in order to maintain the operation of protection components on the organization's network.
- Time limits for execution of critical administrative operations on the organization's network. Critical administrative operations include, for example, distribution of updates for anti-virus databases and modification of policies for client devices.

When selecting a protection structure, it is recommended first to estimate the available network and hardware resources that can be used for the operation of a centralized protection system.

To analyze the network and hardware infrastructure, the following procedure is recommended:

1. Define the following settings of the network on which the protection will be deployed:
   - Number of network segments.
   - The speed of communication channels between individual network segments.
   - Number of managed devices in each of the network segments.
   - Throughput of each communication channel that can be allocated to maintain the operation of the protection.
2. Determine the maximum allowed time for the execution of key administrative operations for all managed devices.
3. Analyze information from (1) and (2), as well as data from load testing of the administration system (see section "Network load" on page 161). Based on the analysis, answer the following questions:
   - Is it possible to hold all the clients with a single Administration Server, or a hierarchy of Administration Servers is required?
   - Which hardware configuration of Administration Servers is required in order to deal with all the clients within the time limits specified in item 2?
   - Is it required to use update agents to reduce workload on communication channels?

Upon obtaining answers to the above-listed questions, you can compile a set of allowed structures of the organization's protection.

On the organization's network you can use one of the following standard protection structures:

- One Administration Server. All client devices are connected to a single Administration Server. Administration Server functions as update agent.
- One Administration Server with update agents. All client devices are connected to a single Administration Server. Some of the networked client devices act as update agents.
- Administration Servers hierarchy. For each of the network segments an individual Administration Server is allocated, making part of a general hierarchy of Administration Servers. The master Administration Server functions as update agent.
- Hierarchy of Administration Servers with update agents. For each of the network segments an individual Administration Server is allocated, making part of a general hierarchy of Administration Servers. Some of the networked client devices act as update agents.

Typical schemes of protection system deployment

This section describes standard deployment schemes of a protection system on an enterprise network using Kaspersky Security Center.

The system must be protected against any types of unauthorized access. We recommend that you install all available security updates for your operating system before you install the application on your device.

You can deploy a protection system on a corporate network using Kaspersky Security Center, by resorting to the following deployment schemes:

- Deploying a protection system via Kaspersky Security Center, by using one of the following methods:
  - Through Administration Console
  - Through Kaspersky Security Center 10 Web Console

  Kaspersky Lab applications are automatically installed on client devices, which, in their turn, are automatically connected to the Administration Server through Kaspersky Security Center.

  The basic deployment scheme is protection system deployment via Administration Console. Using Kaspersky Security Center 10 Web Console allows you to start installation of Kaspersky Lab applications from your browser.
- Deploying a protection system manually using stand-alone installation packages created in Kaspersky Security Center.

  Installation of Kaspersky Lab applications on client devices and the administrator's workstation is performed manually; the settings for connection of client devices to the Administration Server are defined during Network Agent installation.

  This deployment method is recommended to use in case remote installation is impossible.

Kaspersky Security Center also allows deploying a protection system using group policies of Active Directory®. For more details please refer to the Kaspersky Security Center Full Help.

Deploying a protection system within an organization

This section describes processes of protection system deployment within an enterprise that correspond to the standard deployment schemes.

In this section:

Deploying a protection system via Administration Console within an organization 41

Deploying a protection system through Kaspersky Security Center 10 Web Console within an organization 42

Deploying a protection system manually within an organization..... 43

Deploying a protection system via Administration Console within an organization

Remote installation of required software is performed by the administrator of Kaspersky Security Center (hereinafter also referred to as the administrator) via Administration Console. In this case, the deployment process comprises the following basic steps:

1. The administrator deploys the Administration Server as follows:
    a. Installs Kaspersky Security Center on a selected device
    b. Installs Administration Console on the administrator's workstation (if necessary)
    c. Adjusts the Administration Server settings
2. If necessary, the administrator creates the Administration Servers hierarchy in Kaspersky Security Center.

3. The administrator creates a structure of administration groups and distributes client devices of the organization by administration groups.

4. In Kaspersky Security Center, the administrator creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

5. In Administration Console, the administrator selects devices on which the relevant applications need to be installed.

6. The administrator creates and runs remote installation tasks for selected applications through the Administration Console.

7. If necessary, the administrator performs additional configuration of installed applications via Administration Console using policies and local settings of applications.

Deploying a protection system using Kaspersky Security Center 10 Web Console within an organization

Remote installation of required software through Kaspersky Security Center 10 Web Console is performed by the Kaspersky Security Center administrator (hereinafter also referred to as the administrator). In this case, the deployment process comprises the following basic steps:

1. The administrator deploys the Administration Server as follows:

    a. Installs Kaspersky Security Center on a selected device

    b. Installs Kaspersky Security Center 10 Web Console on the same device

    c. Installs Administration Console on the administrator's workstation (if necessary)

    d. Configures Administration Server for work with Kaspersky Security Center 10 Web Console

2. The administrator creates a virtual Administration Server in Kaspersky Security Center in order to manage client devices.

3. The administrator selects a networked computer that should act as update agent, and installs Network Agent on it locally.

   As a result, Kaspersky Security Center automatically assigns the device with Network Agent installed to act as update agent and configures it as connection gateway at the first connection with the Administration Server.

4. On the virtual Administration Server the administrator creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

5. The administrator starts Kaspersky Security Center 10 Web Console.

6. In Kaspersky Security Center 10 Web Console, the administrator starts installation of selected applications on devices.

7. If necessary, the administrator performs additional configuration of installed applications via Administration Console using policies and local settings of applications.

Deploying a protection system manually within an organization

Manual installation of required software with stand-alone installation packages is performed by the administrator of Kaspersky Security Center (hereinafter also referred to as the administrator). In this case, the deployment process comprises the following basic steps:

1. The administrator deploys the Administration Server as follows:

   a. Installs Kaspersky Security Center on a selected device

   b. Installs Administration Console on the administrator's workstation (if necessary)

   c. Adjusts the Administration Server settings

2. If necessary, the administrator creates the Administration Servers hierarchy in Kaspersky Security Center.

3. The administrator creates a structure of administration groups.

4. In Kaspersky Security Center, the administrator creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

5. The administrator creates stand-alone installation packages for the selected applications.

6. The administrator transfers the stand-alone installation packages to client devices by, for example, publishing a link to those installation packages.

7. Users of client devices start installation through the stand-alone installation packages that they received.

8. After the client devices are connected to the Administration Server, they are moved to the respective administration groups specified in the properties of stand-alone installation packages.

Deploying a protection system on a client organization's network

This section describes processes of protection system deployment on a client organization's network that correspond to the standard deployment schemes.

In this section:

Deploying a protection system using Administration Console on a client organization's network 45

Deploying a protection system using Kaspersky Security Center 10 Web Console on a client organization's network..... 46

Deploying a protection system on a client organization's network manually 47

Deploying a protection system using Administration Console on a client organization's network

Remote installation of required software is performed by the administrator of Kaspersky Security Center (hereinafter also referred to as the administrator) via Administration Console. In this case, the deployment process comprises the following basic steps:

1. The administrator of Kaspersky Security Center deploys Administration Server as follows:
    a. Installs Kaspersky Security Center on a selected device
    b. Installs Kaspersky Security Center 10 Web Console on the same device
    c. Installs Administration Console on the administrator's workstation (if necessary)
    d. Configures Administration Server for work with Kaspersky Security Center 10 Web Console
2. The Kaspersky Security Center administrator creates a virtual Administration Server in Kaspersky Security Center to manage client devices in the client organization.

3. The Kaspersky Security Center administrator chooses a device in the organization's network that should act as update agent, and locally installs Network Agent on it.

   As a result, Kaspersky Security Center automatically assigns the client device on which Network Agent is installed to act as update agent and configures it to function as connection gateway at the first connection with the Administration Server.

4. On the virtual Administration Server, the administrator of Kaspersky Security Center creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

5. In Administration Console, the Kaspersky Security Center administrator chooses devices on which the selected applications must be installed.

6. The administrator creates and runs remote installation tasks for selected applications through the Administration Console.

7. If necessary, the administrator performs additional configuration of installed applications via Administration Console using policies and local settings of applications.

Deploying a protection system using Kaspersky Security Center 10 Web Console on a client's corporate network

Remote installation of required software through Kaspersky Security Center 10 Web Console is performed concurrently by the Kaspersky Security Center administrator and the client organization administrator. In this case, the deployment process comprises the following basic steps:

1. The administrator of Kaspersky Security Center deploys Administration Server as follows:

   a. Installs Kaspersky Security Center on a selected device.

   b. Installs Kaspersky Security Center 10 Web Console on the same device.

   c. Installs Administration Console on the administrator's workstation (if necessary).

   d. Configures Administration Server for work with Kaspersky Security Center 10 Web Console.

2. The Kaspersky Security Center administrator creates a virtual Administration Server in Kaspersky Security Center to manage client devices in the client organization.

3. The administrator of the client organization chooses the networked device that will act as update agent, and locally installs Network Agent on it.

   As a result, Kaspersky Security Center automatically assigns the client device on which Network Agent is installed to act as update agent and configures it to function as connection gateway at the first connection with the Administration Server.

4. On the virtual Administration Server, the administrator of Kaspersky Security Center creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

5. In Kaspersky Security Center 10 Web Console, the administrator of the client organization starts installation of the selected applications on client devices.

6. If necessary, the administrator of Kaspersky Security Center performs additional configuration of installed applications via Administration Console using policies and local settings of applications.

Deploying a protection system on a client organization's network manually

Manual installation of required software using stand-alone installation packages is performed concurrently by the administrator of Kaspersky Security Center and the administrator of the client organization. In this case, the deployment process comprises the following basic steps:

1. The administrator of Kaspersky Security Center deploys Administration Server as follows:

   a. Installs Kaspersky Security Center on a selected device.

   b. Installs Kaspersky Security Center 10 Web Console on the same device.

   c. Installs Administration Console on the administrator's workstation (if necessary).

   d. Configures Administration Server for work with Kaspersky Security Center 10 Web Console.

2. The Kaspersky Security Center administrator creates a virtual Administration Server in Kaspersky Security Center to manage client devices in the client organization.

3. The administrator of the client organization chooses the networked device that will act as update agent, and locally installs Network Agent on it.

   As a result, Kaspersky Security Center automatically assigns the client device on which Network Agent is installed to act as update agent and configures it to function as connection gateway at the first connection with the Administration Server.

4. On the virtual Administration Server, the administrator of Kaspersky Security Center creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

5. The administrator of Kaspersky Security Center creates stand-alone installation packages for selected applications.

6. The Kaspersky Security Center administrator sends the stand-alone installation package to the client organization (for example, by publishing a link to that package in Kaspersky Security Center 10 Web Console).

7. The administrator of the client organization sends the stand-alone package to selected devices through Kaspersky Security Center 10 Web Console.

8. Users of client devices start the application installation through a stand-alone installation package.

9. After a client device is connected to the Administration Server, it is moved to the administration group specified in the stand-alone installation package properties.

Deploying Administration Server

This section describes stages of Administration Server deployment.

Deployment stages are described for two different scenarios of managing the application:

- Administration Server deployment within an organization.
- Administration Server deployment for protection of a client organization's network.

> If you need to deploy Administration Server within an organization that includes remote offices not covered by the client organization's network, you can use the protection system deployment scenario for service providers.

Kaspersky Security Center supports integration with Microsoft's Network Access Protection (NAP) that allows you to manage client device access to the network. To check the operating system's operability when running Kaspersky Security Center concurrently with Microsoft NAP, you must additionally install the System Health Validator component (see section "Installing and configuring Kaspersky Security Center SHV" on page 80).

This section then describes actions included in the listed steps of protection deployment.

In this section:

Stages of deploying Administration Server within an enterprise 50

Steps of Administration Server deployment for protection of a client organization's network 50

Upgrading Kaspersky Security Center 50

Installing and removing Kaspersky Security Center 52

Installing Administration Console on the administrator's workstation 78

Configuring the connection of Administration Console to Administration Server 79

Installing and configuring Kaspersky Security Center SHV 80

Installing Kaspersky Security 10 Center Web Console 82

Advanced configuration of Kaspersky Security Center 10 Web Console and Self Service Portal 88

Stages of deploying Administration Server within an enterprise

► *To deploy Administration Server within an organization:*

1. Install the Kaspersky Security Center on the administrator's workstation.
2. Configure the Administration Server settings.

Steps of Administration Server deployment for protection of a client organization's network

► *To deploy Administration Server for protection of a client organization's network:*

1. Install the Kaspersky Security Center on the administrator's workstation.
2. Install Kaspersky Security Center 10 Web Console on the administrator workstation.
3. Configure Administration Server for cooperation with Kaspersky Security Center 10 Web Console.

Upgrading Kaspersky Security Center

You can install Administration Server 10 on a device with an earlier version of Administration Server installed. When you upgrade Administration Server to version 10, all data and settings from the previous version of the application are saved.

Before upgrading Kaspersky Security Center, you have to decrypt all encrypted drives of devices on which application components (Administration Servers, Network Agents) are installed. When Kaspersky Security Center is upgraded, decrypted disks can be re-encrypted.

► *To upgrade Administration Server of the 9.0 version to the 10 version:*

1. Run the executable file setup.exe for the version 10.

   A window opens prompting you to select Kaspersky Lab applications to install.

   In the application selection window, click the **Install Kaspersky Security Center Administration Server** link to run the Administration Server Setup Wizard. Follow the instructions of the Wizard.

2. Read the License Agreement concluded between you and Kaspersky Lab. If you agree with all of its terms, select the **I accept the terms of the License Agreement** check box.

   Installation of the application then continues. The Setup Wizard prompts you to create a backup copy of the data of Kaspersky Security Center 9.0 Administration Server.

   Kaspersky Security Center supports data recovery from a backup copy of Administration Server created by an older version of the application.

3. If you need to create a backup copy, in the **Administration Server Backup** window that opens, select the **Create backup copy of Administration Server** check box.

   A backup copy of Administration Server data is created by the klbackup utility. This utility is included in the application distribution, and is located in the root of the Kaspersky Security Center installation folder.

   For details on the operation of the data backup and recovery utility, refer to the Kaspersky Security Center Full Help, "Applications" section.

4. Install Administration Server version 10, following the Setup Wizard's instructions.

   We recommend that you avoid aborting the Setup Wizard operation.
   Canceling the product setup at the step of Administration Server installation may cause Kaspersky Security Center 9.0 to fail.

5. For devices with an earlier version of Network Agent installed, create and run the remote installation task for the new version of Network Agent (see section "Installing applications using the remote installation task" on page 100).

   After completing the remote installation task, the Network Agent version will be upgraded.

If problems occur during Administration Server installation, you can restore the previous version of Administration Server using the backup copy of the Administration Server data created before the upgrade.

If at least one Administration Server of the new version has been installed in the network, other Administration Servers in the network can be upgraded using the remote installation task that uses the Administration Server installation package.

Installing and removing Kaspersky Security Center

This section describes local installation of Kaspersky Security Center components. Two installation options are available:

- **Standard**. The minimum required set of components will be installed in this case. This type of installation is recommended for networks that contain up to 200 devices.
- **Custom**. In this case, you can select specific components for installation and adjust additional application settings. This type of installation is recommended for networks that contain more than 200 devices. Custom installation is recommended for experienced users.

If at least one Administration Server is installed in the network, Servers can be remotely installed on other networked devices through the remote installation task using forced installation (see section "Installing applications using a remote installation task" on page 100). When creating the remote installation task, you should use the Administration Server installation package.

In this section:

Preparing for installation 53

Standard installation 56

Custom installation 57

Installation in non-interactive mode 67

Changes in the system after installing the application 74

Removing the application 77

Preparing for installation

Before starting installation, make sure that the device's hardware and software meets the requirements for Administration Server and Administration Console.

Kaspersky Security Center stores its information in a SQL Server database. Therefore, by default, Microsoft SQL Server 2014 Express SP1 is installed together with Kaspersky Security Center. Other SQL servers can be used for storing data. In that case they must be installed on the network before the start of installation of Kaspersky Security Center.

Kaspersky Security Center installation requires administrator privileges on the device on which the installation is planned.

To ensure that the application components function properly after setup, all the required ports must be open on devices (see table below).

Table 4. Ports used by Kaspersky Security Center

Port number	Protocol	Description
Device with Administration Server installed		
8060	HTTP	Used for connection to Web Server for the Kaspersky Security Center 10 Web Console operation, and for the enterprise intranet administration.
8061	HTTPS	Used for connection to Web Server for the Kaspersky Security Center 10 Web Console operation, and for the enterprise intranet administration. This connection type uses encryption.
13000	TCP	Used to: • Retrieve data from client devices. • Connect to update agents. • Connect to slave Administration Servers. SSL protection is used for these connections.
13000	UDP	Used to report on device shutdown.
13111	TCP	Used for connecting to a KSN server.
13291	TCP	Used for connecting Administration Console to Administration Server. SSL protection is used for these connections.
13292	TCP	This port is used for connections with mobile devices.

Port number	Protocol	Description
14000	TCP	Used to: • Retrieve data from client devices. • Connect to update agents. • Connect to slave Administration Servers. SSL protection is not used for these connections.
17000	TCP	Used for connecting to an activation proxy server. SSL protection is used for these connections.
17100	TCP	Used for connecting to an activation proxy server in order to activate mobile clients.
Device assigned to act as update agent		
13000	TCP	The port is used by client devices to connect to the update agent.
13001	TCP	The port is used by client devices to connect to the update agent if a device with Administration Server installed acts as update agent.
14000	TCP	The port is used by client devices to connect to the update agent.
14001	TCP	The port is used by client devices to connect to the update agent if a device with Administration Server installed acts as update agent.
Client device with Network Agent installed		
7	UDP	The port is used by the Wake On LAN feature.
9	UDP	
67	UDP	The port is used on the device that has been assigned to act

Port number	Protocol	Description
69	UDP	as PXE server, when deploying operating system images.
15,000	UDP	The port is used to receive requests for connection to the Administration Server, which allows to receive information about a device in real-time mode.
15001	UDP	Used to interact with the update agent.

Client devices use 1024—5000 (TCP) as the range of ports for their outbound connections with the Administration Server and update agents. In Microsoft Windows Vista and Microsoft Windows Server 2008 the default range of ports for outbound connections is 49152–65535 (TCP).

Standard installation

► *To perform standard installation of Kaspersky Security Center on a local device:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

   In the application selection window, click the **Install Kaspersky Security Center Administration Server** link to run the Administration Server Setup Wizard. Follow the instructions of the Wizard.

2. Read the License Agreement concluded between you and Kaspersky Lab. If you agree with all of its terms, select the **I accept the terms of the License Agreement** check box. Installation of the application then continues.

   The Setup Wizard may also prompt you to view the License Agreements for application management plug-ins available from the Kaspersky Security Center distribution kit, and to accept the terms of those License Agreements.

3. Select **Standard** and click the **Next** button.

The Setup Wizard extracts the necessary files from the distribution package and writes them to the hard drive of the device.

On the last page the Setup Wizard invites you to start Administration Console. When the Console starts for the first time, you can perform initial configuration of the application (for details, please refer to the *Kaspersky Security Center Administrator's Guide*).

When the Setup Wizard finishes, the following application components are installed on the hard drive on which the operating system has been installed:

- Administration Server (together with the server version of Network Agent).
- Administration Console.
- Application management plug-ins available in the distribution kit.

The following applications are also installed, if they have not been installed previously:

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

Custom installation

► *To perform custom installation of Kaspersky Security Center on a local device:*

Run the setup.exe executable file.

A window opens prompting you to select Kaspersky Lab applications to install. In the application selection window, click the **Install Kaspersky Security Center Administration Server** link to run the Administration Server Setup Wizard. Follow the instructions of the Wizard.

The following text describes the steps of the Setup Wizard and actions that you can perform at each step.

The wizard's steps

Step 1. Reviewing the License Agreement 58

Step 2. Selecting an installation method 59

Step 3. Selecting the components to be installed 59

Step 4. Selecting network size 60

Step 5. Selecting an account 61

Step 6. Configuring an account to run services 62

Step 7. Selecting a database 62

Step 8. Configuring SQL Server 62

Step 9. Selecting an authentication mode 64

Step 10. Selecting a shared folder 65

Step 11. Configuring the connection to Administration Server 65

Step 12. Defining the Administration Server address 66

Step 13. Configuring settings for mobile devices 66

Step 14. Selecting application management plug-ins 66

Step 15. Unpacking and installing files on the hard drive 67

Step 1. Reviewing the License Agreement

At this step of the Setup Wizard, you should read the License Agreement, which is to be concluded between you and Kaspersky Lab.

You may also be prompted to view the License Agreements for application management plug-ins that are available in the Kaspersky Security Center distribution kit.

Please, read the End User License Agreement carefully. If you accept all of the provisions, select the **I accept the terms of the License Agreement** check box. Installation continues.

If you do not accept the End User License Agreement, cancel installation by clicking the **Cancel** button.

Step 2. Selecting an installation method

Select the **Custom** installation method.

Step 3. Selecting the components to be installed

Select the components of Kaspersky Security Center Administration Server that you want to install:

- **Mobile device support**. This component ensures management of mobile device protection through Kaspersky Security Center.
- **SNMP agent**. This component retrieves statistical information for the Administration Server over the SNMP protocol. The component is available if the application is installed on a device with SNMP installed.

  > After Kaspersky Security Center is installed, the .mib files required for retrieving statistics are located in the SNMP subfolder of the application installation folder.

The Wizard window contains reference information about the selected component and the disk space required for installation.

Network Agent and Administration Console are not displayed in the component list. These components are installed automatically and you cannot cancel their installation.

> The server version of Network Agent is installed on the device together with Administration Server. Administration Server cannot be installed together with the regular version of Network Agent. If the server version of Network Agent is already installed on your device, remove it and start Administration Server installation again.

At this step you must specify a folder for installation of Administration Server components. By default, the components are installed to <Disk>:\Program Files\Kaspersky Lab\Kaspersky

Security Center. If no such folder exists, this folder is created automatically during installation. You can change the destination folder by using the **Browse** button.

Step 4. Selecting network size

Specify the size of the network on which Kaspersky Security Center is being installed. Depending on the number of devices in the network, the Wizard configures installation and appearance of the application interface.

The following table lists the application installation settings and interface appearance settings that are adjusted based on various network sizes.

Table 5. Dependence of installation settings on the network scale selected

Settings	1 through 100 devices	101 through 1000 devices	1001 through 5000 devices	5001+ devices
Display of node for slave and virtual Administration Servers and all settings related to slave and virtual Administration Servers in the console tree	not available	not available	available	available
Display of **Security** sections in the properties windows of the Administration Server and administration groups	not available	not available	available	available
Random distribution of startup time for the update task on client devices	not available	over interval of 5 minutes	over interval of 10 minutes	over interval of 10 minutes

If you connect Administration Server to a MySQL or SQL Express database server, we recommend that you avoid to use the application to manage more than 5,000 devices.

Step 5. Selecting an account

Select the account that will be used to start Administration Server as a service on the device:

- **Local System Account**. Administration Server will start under the *Local System Account*, using the credentials of that account.

  For proper functioning of Kaspersky Security Center, the account used to start Administration Server must have administrator rights on the resource on which the Administration Server database is hosted.

  In Microsoft Windows Vista and later versions of Microsoft Windows, Administration Server cannot be installed under the local system account. In these cases, the **Automatically generated account (<Account name>)** option is available.

- **User account**. The Administration Server will start under the selected user account. Administration Server will initiate all operations by using the credentials of that account. Click the **Select** button to select the user account and specify password.

When using an SQL server in a mode that presupposes authenticating user accounts with Microsoft Windows tools, access to the database should be granted. The user account must have the status of owner of the Kaspersky Anti-Virus database. The dbo schema is used by default.

If later you decide to change the Administration Server account, you can use the utility for Administration Server account switching (*klsrvswch*). For more details please refer to the *Kaspersky Security Center Administrator's Guide*.

Step 6. Configuring an account to run services

Select the user account under which Kaspersky Security Center services will be run on this device:

- **Automatically generated account**. Kaspersky Security Center creates an account in the kladmins group. The services of Kaspersky Security Center will be run under the account that has been created.
- **Specify an account**. The services of Kaspersky Security Center will be run under the user account that has been specified. Click the **Select** button to specify a user account and enter the password.

Step 7. Selecting a database

At this step of the Wizard, you must select the mechanism – Microsoft SQL Server (SQL Express) or MySQL – that will be used to store the Administration Server database.

> If you install Kaspersky Security Center on a server that acts as a read-only domain controller (RODC), Microsoft SQL Server (SQL Express) is not available for installation. In this case, to install Kaspersky Security Center properly, we recommend that you use MySQL.

The Administration Server database structure is provided in the file klakdb.chm, which is located in the Kaspersky Security Center installation folder.

Step 8. Configuring SQL Server

At this step of the Wizard, the SQL server is configured.

Depending on the database that you have selected, the following options are available for SQL server configuration:

- If you have selected SQL Express or Microsoft SQL Server during the previous step, select one of the following options:
  - If an SQL server is installed on the enterprise network, specify its name in the **SQL Server name** field.

The **SQL Server name** field displays the name of an SQL Server by default if one is detected on the device from which Kaspersky Security Center is to be installed. To view a list of all SQL Servers that are installed on the network, clicking the **Browse** button.

> If Administration Server starts under a local administrator or local system account, the **Browse** button is not available.

In the **Database name** field, specify the name of the database that will be created for storing Administration Server data. The default name for the database is **KAV**.

> If you intend to manage fewer than 5,000 devices through Kaspersky Security Center, you can use Microsoft SQL Express 2005/2008. If you intend to manage more than 5,000 devices through Kaspersky Security Center, we recommend that you use Microsoft SQL 2005/2008.

> We recommend that you use any SQL Server edition other than Express if you intend to use Application Privilege Control to manage more than 50 devices.

- If SQL Server is not installed on the network, select the option **Install Microsoft SQL Server 2014 Express SP1**.

  The Setup Wizard then installs Microsoft SQL Server 2014 Express SP1. The necessary settings are configured automatically.

- If a MySQL Server was selected at the previous step, specify its name in the **SQL Server name** field (by default, the system uses the IP address of the device on which Kaspersky Security Center is to be installed). In the **Port** field, specify the connection port (the default port number is 3306).

  In the **Database name** field, enter the name of the database that will be created for storing Administration Server data (the default database name is **KAV**).

If you want to install SQL Server manually on the device from which you are running Kaspersky Security Center installation, you must abort installation and restart it after SQL Server installation. The supported SQL servers are listed in the system requirements.

If you want to install SQL server on a remote device manually, there is no need to abort the Kaspersky Security Center Setup Wizard. Install SQL Server and return to installation of Kaspersky Security Center.

Step 9. Selecting an authentication mode

Determine the authentication mode that will be used when Administration Server connects to the SQL Server.

Depending on the database that is selected, you can choose from among the following authentication modes.

- For SQL Express or Microsoft SQL Server select one of the following options:
  - **Microsoft Windows Authentication Mode**. Verification of rights uses the account used for starting Administration Server.
  - **SQL Server Authentication Mode**. If you select this option, the account specified in the window is used to verify access rights. Fill in the **Account**, **Password** and **Confirm password** fields.

  If the Administration Server database is on another device and the Administration Server account has no access to the database server, you have to use the SQL Server authentication mode during Administration Server installation or upgrade. This may occur when the device storing the database is outside the domain or when Administration Server is installed under a local system account.
- Specify the user account and password for MySQL Server.

Step 10. Selecting a shared folder

Define the location and name of the shared folder that will be used to do the following:

- Store the files necessary for remote installation of applications (these files are copied to Administration Server during creation of installation packages).
- Store updates that have been downloaded from an update source to Administration Server.

File sharing (read-only) will be enabled for all users.

You can select either of the following options:

- **Create a shared folder**. Create a new folder. In the text box, specify the path to the folder.
- **Select existing shared folder**. Select a shared folder that already exists.

The shared folder can be a local folder on the device from which you are running installation, or it can be a remote folder on any client device in the corporate network. You can click the **Browse** button to select the shared folder, or specify the shared folder manually by entering its UNC path (for example, \\server\Share) in the corresponding field.

By default, the installer creates a local Share subfolder in the application folder that contains the components of Kaspersky Security Center.

Step 11. Configuring the connection to Administration Server

Configure the connection to Administration Server:

- **Port number**. Port number to connect to Administration Server. The default port number is 14000.
- **SSL port number**. Port number to connect to Administration Server by using SSL protocol. The default port number is 13000.

If Administration Server is installed on a computer running on Microsoft Windows XP with Service Pack 2, the built-in system firewall blocks TCP ports 13000 and 14000. Therefore, to allow access to Administration Server on the device after installation, you have to open these ports manually.

Step 12. Defining the Administration Server address

Specify the Administration Server address. You can select one of the following options:

- **DNS domain name**. This method is helpful if the network includes a DNS server and client devices can use it to retrieve the Administration Server address.
- **NetBIOS name**. This method is helpful if client devices retrieve the Administration Server address via NetBIOS or if a WINS Server is in the network.
- **IP address**. This option is used if Administration Server has a static IP address that will not be subsequently changed.

Step 13. Configuring settings for mobile devices

This Setup Wizard step is available if you have selected the **Mobile device support** component for installation.

Specify the Administration Server address for mobile device connections.

Step 14. Selecting application management plug-ins

Select the application management plug-ins that need to be installed with Kaspersky Security Center.

Step 15. Unpacking and installing files on the hard drive

After the installation of Kaspersky Security Center components is configured, you can start installing files on the hard drive.

If installation requires additional programs, the Setup Wizard will notify you, in the **Installing Prerequisites** window, before installation of Kaspersky Security Center. The required programs are installed automatically after you click the **Next** button.

Installation in non-interactive mode

Kaspersky Security Center can be installed in non-interactive mode, which does not require interactive input of installation settings by the user.

► *To install Kaspersky Security Center on a local device in non-interactive mode:*

run the command

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

where `setup_parameters` is a list of settings and their respective values, separated with spaces (`PRO1=PROP1VAL PROP2=PROP2VAL`). Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center in the Server folder.

Names and possible values for settings that can be used when installing Administration Server in non-interactive mode are listed in the table below.

Table 6. Settings of Administration Server installation in non-interactive mode

Setting name	Setting description	Available values
EULA	Acceptance of the terms of the License Agreement	• 1 – I accept the terms of the License Agreement • Other value, or no value – I do not accept the terms of the License Agreement (installation is not performed)

Setting name	Setting description	Available values
INSTALLATIONMODETYPE	Type of Administration Server installation	• Standard – standard installation • Custom – custom installation
INSTALLDIR	Path to the Administration Server installation folder	String value
ADDLOCAL	List of Administration Server components (separated with commas) to be installed	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86 Minimum list of components sufficient for proper Administration Server installation: `ADDLOCAL=CSAdminKitServer,CSAdminKitConsole,KSNProxy,Microsoft_VC90_CRT_x86,Microsoft_VC100_CRT_x86`
NETRANGETYPE	Network size (number of networked devices)	• NRT_1_100—From 1 to 100 devices • NRT_100_1000—From 101 to 1000 devices • NRT_GREATER_1000—1001+ devices

Setting name	Setting description	Available values
SRV_ACCOUNT_TYPE	Mode for specifying the account under which Administration Server will be run as a service	• SrvAccountDefault – the account is created automatically • SrvAccountUser – the account is created manually; in this case, you must specify values for the SERVERACCOUNTNAME and SERVERACCOUNTPWD settings
SERVERACCOUNTNAME	Name of the account under which Administration Server will be run as a service; you must specify a value for the setting if SRV_ACCOUNT_TYPE=SrvAccountUser	String value
SERVERACCOUNTPWD	Password of the account under which Administration Server will be run as a service; you must specify a value for the setting if SRV_ACCOUNT_TYPE=SrvAccountUser	String value
SERVERCER	Size of the key for the Administration Server certificate (bits)	• 1 – the size of the key for the Administration Server certificate is 2,048 bits • No value specified – the size of the key for the Administration Server certificate is 1,024 bits

Setting name	Setting description	Available values
DBTYPE	Type of database that will be created to store the Administration Server database.	• MySQL – MySQL database will be used; in this case, you must specify values for the MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME, and MYSQLACCOUNTPWD settings • MSSQL – Microsoft SQL Server (SQL Express) database will be used; in this case, you must specify values for the MSSQLCONNECTIONTYPE and MSSQLAUTHTYPE settings
MYSQLSERVERNAME	Full name of the SQL server; you must specify a value for the setting if DBTYPE=MySQL	String value
MYSQLSERVERPORT	Number of the port for connecting to the SQL server; you must specify a value for the setting if DBTYPE=MySQL	String value
MYSQLDBNAME	Name of the database that will be created to store Administration Server data; you must specify a value for the setting if DBTYPE=MySQL	String value

Setting name	Setting description	Available values
MYSQLACCOUNTNAME	Name of the account for connecting to the database; you must specify a value for the setting if DBTYPE=MySQL	String value
MYSQLACCOUNTPWD	Password of the account for connecting to the database; you must specify a value for the setting if DBTYPE=MySQL	String value
MSSQLCONNECTIONTYPE	Type of use of the MSSQL database; you must specify a value for the setting if DBTYPE=MSSQL	• InstallMSSEE – install Microsoft SQL Server 2014 Express SP1; all the required settings will be defined automatically • ChooseExisting – use an SQL server installed on the enterprise network; in this case, you must specify values for the MSSQLSERVERNAME and MSSQLDBNAME settings
MSSQLSERVERNAME	Full name of the SQL server; you must specify a value for the setting if MSSQLCONNECTIONTYPE=ChooseExisting	String value

Setting name	Setting description	Available values
MSSQLDBNAME	Name of the database; you must specify a value for the setting if MSSQLCONNECTIONTYPE=ChooseExisting	String value
MSSQLAUTHTYPE	Type of authorization when connecting to the SQL server; you must specify a value for the setting if DBTYPE=MSSQL	• Windows – Microsoft Windows authentication mode • SQLServer – SQL server authentication mode; in this case, you must specify values for the MSSQLACCOUNTNAME and MSSQLACCOUNTPWD settings
MSSQLACCOUNTNAME	Name of the account for connection to the SQL server; you must specify a value for the setting if MSSQLAUTHTYPE=SQLServer	String value
MSSQLACCOUNTPWD	Password of the account for connection to the SQL server; you must specify a value for the setting if MSSQLAUTHTYPE=SQLServer	String value

Setting name	Setting description	Available values
CREATE_SHARE_TYPE	Method of specifying the shared folder	• Create – create a new shared folder; in this case, you must specify values for the SHARELOCALPATH and SHAREFOLDERNAME settings • ChooseExisting – select an existing folder; in this case, you must specify a value for the EXISTSHAREFOLDERNAME setting
SHARELOCALPATH	Full path to a local folder; you must specify a value for the setting if CREATE_SHARE_TYPE=Create	String value
SHAREFOLDERNAME	Network name of a shared folder; you must specify a value for the setting if CREATE_SHARE_TYPE=Create	String value
EXISTSHAREFOLDERNAME	Full path to an existing shared folder; you must specify a value for the setting if CREATE_SHARE_TYPE=ChooseExisting	String value

Setting name	Setting description	Available values
SERVERPORT	Port number to connect to Administration Server.	Numerical value
SERVERSSLPORT	Port number to connect to Administration Server by using SSL protocol.	Numerical value
SERVERADDRESS	Administration Server address	String value
MOBILESERVERADDRESS	Administration Server address for connections with mobile devices	String value

For a detailed description of Administration Server installation settings, please refer to the "**Custom installation"** section (see page 57).

Changes in the system after installing the application

After Administration Console is installed on your device, its icon appears and can be used to start the Console. Click **Start** → **Programs** → **Kaspersky Security Center**.

Administration Server and Network Agent are installed on the device as services with the properties listed below. The table also contains the attributes of other services that apply on the device after Administration Server installation.

Table 7. Service attributes

Component	Service name	Displayed service name	Startup type	Account
Administration Server	kladminserver	Kaspersky Security Center Administration Server	Automatically when the operating system starts up	User-defined or dedicated account (of the format KL-AK-*, created during installation)
Network Agent	klnagent	Kaspersky Security Center Network Agent	Automatically when the operating system starts up	Local system
Web server for accessing Web Console and administering the enterprise's intranet	klwebsrv	Kaspersky Lab web server	Automatically when the operating system starts up	Dedicated unprivileged account in KlScSvc-* format
Activation proxy server	klactprx	Kaspersky Lab activation proxy server	Automatically when the operating system starts up	Dedicated unprivileged account in KlScSvc-* format
Web access authorization portal	klnsacwsrv	Kaspersky Lab authorization portal	Manually	Local system

Component	Service name	Displayed service name	Startup type	Account
KSN proxy server	ksnproxy	Kaspersky Security Network proxy server	Manually	Dedicated unprivileged account in KlScSvc-* format
iOS MDM Server	KLIOSMdmServiceSrv2	iOS MDM Server	Automatically when the operating system starts up	Network Service
COM+ object for interaction with Exchange server	KasperskyMdmService	Kaspersky MDM for Exchange	Automatically when calling an object	User account included in the Domain User and KLMDM Role Group (KLMDM Secure Group) groups

The server version of Network Agent will be installed on the device together with Administration Server. The server version of Network Agent is part of Administration Server, is installed and removed together with Administration Server, and can only interact with a locally installed Administration Server. You do not have to configure the Network Agent connection to the Administration Server; the configuration is implemented through program features because the components are installed on the same device. Also, the connection settings will not be available through the local settings of Network Agent on that device. Such a configuration helps avoid additional setting customization and potential conflicts in the operation of these components when they are installed separately.

The server version of Network Agent is installed with the same properties as the standard Network Agent and performs the same application management functions. This version will be affected by the policy of the administration group to which the Administration Server client device belongs.

For the server version of Network Agent all tasks are created from the scope of those provided for Administration Server, except for the Server change task.

> No individual installation of Network Agent is required on the Administration Server device. Its functions are performed by the server version of the Network Agent.

You can view the properties of each service of the Server, Network Agent, or Kaspersky Lab Policy Server, as well as monitor their operation using standard Microsoft Windows management tools: Computer management\Services. Information about the operation of Kaspersky Lab Administration Server service is stored in the Microsoft Windows system log in a separate Kaspersky Event Log branch on the device with Administration Server installed.

Local groups of users named KLAdmins and KLOperators will also be created automatically on the device with Administration Server installed. If Administration Server starts using an account included in the domain, the KLAdmins and KLOperators user groups are added to the list of domain user groups. The user groups can be modified by using the standard Microsoft Windows administration tools.

> To configure email notifications, the administrator may have to create an account on mail server for ESMTP authentication.

Removing the application

You can remove Kaspersky Security Center using standard Microsoft Windows add/remove tools. To remove the application, a wizard starts that removes all the application components from the device (including plug-ins). If you have not selected removal of the shared folder (Share) during the wizard's operation, you can delete it manually after completion of all related tasks.

The Application Removal Wizard will suggest that you store a backup copy of Administration Server.

> When removing the application from Microsoft Windows 7 and Microsoft Windows 2008, premature termination of the removal wizard might occur. This can be avoided by disabling the User Account Control (UAC) in the operating system and restarting application removal.

Installing Administration Console on the administrator's workstation

You can install Administration Console on the administrator's workstation separately and manage Administration Server over the network using that Console.

► *To install Administration Console on the administrator's workstation:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

   In the application selection window, click the **Install Kaspersky Security Center Administration Console** link to run the Administration Console Setup Wizard. Follow the instructions of the Wizard.

   > The installation of Administration Console from the distribution package downloaded from the Internet does not differ from the installation of Administration Console from the installation CD.

2. Select a destination folder. By default, this will be <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

3. In the last window of the Setup Wizard click the **Start** button to start the Administration Console installation.

   When the Wizard finishes its operations, Administration Console will be installed on the administrator's workstation.

After installing Administration Console, you must connect to the Administration Server. To do this, run Administration Console and, in the window that opens, specify the name or the IP address of the device on which Administration Server is installed, as well as the settings of the user account for connection. After connection to Administration Server is established, you can manage the anti-virus protection system using this Administration Console.

You can remove Administration Console with standard Microsoft Windows add/remove tools.

Configuring the connection of Administration Console to Administration Server

In earlier versions of Kaspersky Security Center, Administration Console was connected to Administration Server via SSL port TCP 13291, as well as SSL port TCP 13000. Starting from Kaspersky Security Center 10 Service Pack 2, the SSL ports used by the application are strongly separated and any misuse of ports is impossible:

- SSL port TCP 13291 can only be used by Administration Console and klakaut automation objects.
- SSL port TCP 13000 can only be used by Network Agent, a slave Administration Server, and the master Administration Server in the DMZ.

Port TCP 14000 can only be used for connecting Administration Console, update agents, slave Administration Servers, and klakaut automation objects, as well as for retrieving data from client devices.

In some cases, Administration Console may need to be connected via SSL port 13000:

- If a single SSL port is likely to be used both for Administration Console and for other activities (retrieving data from client devices, connecting update agents, or connecting slave Administration Servers).
- If a klakaut automation object is not connected to Administration Server directly but via an update agent in the DMZ.

► *To allow the connection of Administration Console via port 13000:*

1. Open the system registry of the device on which Administration Server is installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:
   - For a 64-bit system:

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

- For a 32-bit system:

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

3. For the LP_ConsoleMustUsePort13291 (DWORD) key, set the value on 00000000.

   1 is the default value specified for this key.

4. Restart the Administration Server service.

As a result, you will be able to connect Administration Console to Administration Server via port 13000.

Installing and configuring Kaspersky Security Center SHV

Kaspersky Security Center supports integration with the Microsoft Network Access Protection (NAP). Microsoft NAP allows you to manage client devices' network access. Microsoft NAP assumes that the network includes a dedicated server with Microsoft Windows Server 2008 installed running Posture Validation Server (PVS), and client devices have NAP-compatible operating systems installed, such as Microsoft Windows Vista, Microsoft Windows XP Service Pack 3, or Microsoft Windows 7.

When both Kaspersky Security Center and Microsoft NAP are running, the system performance is checked by System Health Validator (referred to as Kaspersky Security Center SHV).

► *To install Kaspersky Security Center SHV on a device locally:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

In the application selection window, click the **Install Kaspersky Security Center SHV** link to run the Kaspersky Security Center SHV Setup Wizard. Follow the instructions of the Wizard.

> Installation of Kaspersky Security Center SHV from the distribution package downloaded from the Internet is identical to that from the installation CD.

2. Specify the destination folder. By default, this will be <Drive>:\Program Files\Kaspersky Lab\Kaspersky Security Center SHV. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

3. In the last window of the Setup Wizard click the **Start** button to start the installation of Kaspersky Security Center SHV.

After the Wizard completes, Kaspersky Security Center SHV is installed on your device.

You can remove Kaspersky Security Center SHV using standard Microsoft Windows add/remove tools. This starts the Wizard, which removes all the application components from the device.

Installing Kaspersky Security Center 10 Web Console

Administration Console must be installed on the device on which you intend to install Kaspersky Security Center 10 Web Console (see section "Installing Administration Console on the administrator workstation" on page 78).

> On devices running Windows 7, Windows Server 2008, or Windows Vista, the KB2533623 (https://support.microsoft.com/en-us/kb/2533623) update must also be installed.

Kaspersky Security Center 10 Web Console installation requires local administrator rights.

► *To install Kaspersky Security Center 10 Web Console on a local device,*

run the install.exe file from the CD with the Kaspersky Security Center 10 Web Console distribution package.

The corresponding wizard will guide you through the installation. The Setup Wizard prompts you to define the application settings. Follow the instructions of the Wizard.

> Kaspersky Security Center 10 Web Console installation from a distribution package downloaded from the Internet is no different than installation from the installation CD.

The wizard's steps

Step 1. Reviewing the License Agreement 83

Step 2. Connecting to Kaspersky Security Center 84

Step 3. Selecting the destination folder 85

Step 4. Selecting the Apache Server installation mode 85

Step 5. Installing Apache Server 85

Step 6. Selecting the ports 86

Step 7. Selecting an account 86

Step 8. Starting Kaspersky Security Center 10 Web Console installation 86

Step 9. Completing Kaspersky Security Center 10 Web Console installation 87

Upgrading Kaspersky Security Center 10 Web Console..... 87

Step 1. Reviewing the License Agreement

At this step of the Setup Wizard, you should read the License Agreement, which is to be concluded between you and Kaspersky Lab.

Please, read the End User License Agreement carefully. If you accept all of the provisions, select the **I accept the terms of the License Agreement** check box. Installation continues.

If you do not accept the End User License Agreement, cancel installation by clicking the **Cancel** button.

Remote installation of Kaspersky Security Center 10 Web Console through an installation package or local installation in non-interactive mode means automatic acceptance of the terms of the End User License Agreement related to the application that you intend to install.
You can view the End User License Agreement for a specific application in the distribution kit of the application or on the Kaspersky Lab Technical Support website.

Step 2. Connecting to Kaspersky Security Center

Select a method of Kaspersky Security Center 10 Web Console connection to Kaspersky Security Center. The following connection options are available:

- **Use Apache server installed on local device**. If this option is selected, Kaspersky Security Center 10 Web Console connects to Kaspersky Security Center through an Apache server installed on a local device (you can select Apache server installation at the next step of the Wizard).

- **Use Apache server installed on remote device**. You can select this option if an Apache server is already installed on a remote device. In this case, only the server part of Kaspersky Security Center 10 Web Console is installed locally. To connect Kaspersky Security Center 10 Web Console to Kaspersky Security Center, install the client part of Kaspersky Security Center 10 Web Console on a remote device. If you select this option, the Setup Wizard proceeds to Step 8 (see section "Step 8. Starting Kaspersky Security Center 10 Web Console installation" on page 86).

► *To install the client part of Kaspersky Security Center 10 Web Console on a remote device running Linux,*

run one of the following files depending on the type of your system:

- For 32-bit systems:
  - kscwebconsole-10.<build_number>.i386.rpm;
  - kscwebconsole_10.<build_number>_i386.deb.
- For 64-bit systems:
  - kscwebconsole-10.<build_number>.x86_64.rpm;
  - kscwebconsole_10.<build_number>_x86_64.deb.

Step 3. Selecting the destination folder

Specify the destination folder for Kaspersky Security Center 10 Web Console installation. By default, this will be <Drive>:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console. If this folder does not exist, it will be created automatically. You can change the destination folder by using the **Browse** button.

Step 4. Selecting the Apache server installation mode

If no Apache server is installed on the device, at this step, the Setup Wizard prompts you to install Apache HTTP Server 2.4.25.

By default, Apache HTTP Server 2.4.25 is selected as the installation option. If you do not want to install the Apache server through the Kaspersky Security Center 10 Web Console Setup Wizard, clear the **Install Apache HTTP Server 2.4.25** check box.

> Apache Server installation may prompt you to restart the device.

Step 5. Installing Apache Server

At this step of the Wizard, Apache HTTP Server 2.4.25 is installed and configured.

Before installation, specify the certificate that will be used for encryption of the connection between the Apache server and the user browser. Select one of the following options:

- **Generate new certificate**. Create a certificate for working via HTTPS.
- **Choose existing**. Use an existing certificate for working via HTTPS. Specify a certificate using one of the available methods:
  - **Select certificate file**. You can select an existing certificate by clicking the **Browse** button.
  - **Select a private key**. You can specify a certificate using the file of its closed key by clicking the **Browse** button.

Step 6. Selecting the ports

Define the following settings:

- Number of the SSL port for encrypted connection of the device to the Administration Server. The default port number is 13291.
- Number of the port for the device connection to the Apache server. The default port number is 9000.
- Address of the device with Administration Server installed. The default address is localhost.

  If the device on which Kaspersky Security Center 10 Web Console and Self Service Portal are to be installed is in DMZ, select the **Connection gateway** check box and specify the connection gateway address in the **Server address** field.
- Number of the port for the device connection to Kaspersky Security Center 10 Web Console. The default port number is 8080.
- Number of the port for the device connection to Self Service Portal. The default port number is 8081.

When Kaspersky Security Center 10 Web Console and Self Service Portal are installed, you can change the default port numbers (see section "Changing the port number for device connection" on page 88).

Step 7. Selecting an account

Specify the user's domain account under which installation packages will be downloaded to users' mobile devices by means of QR codes. The account must be specified in *<Domain name>\<Account name>* format.

Click the **Test** button to test the Administration Server connection.

Step 8. Starting Kaspersky Security Center 10 Web Console installation

Click the **Start** button to start Kaspersky Security Center 10 Web Console installation.

The installation process is displayed on the Wizard page.

Step 9. Completing Kaspersky Security Center 10 Web Console installation

If Apache Server, version 2.4.25 or later, is already installed on the computer, or if automatic installation of Apache Server returned an error, at this step of the Kaspersky Security Center 10 Web Console Setup Wizard, you are prompted to open the file with instructions on how to configure an Apache server. To open the instructions file, select the **Open readme.txt** check box.

To complete the Setup Wizard, click the **Finish** button.

Upgrading Kaspersky Security Center 10 Web Console

You can install Kaspersky Security Center 10 Web Console on a device on which an earlier version of Kaspersky Security Center 10 Web Console has been installed. When upgrading to version 10, all data and settings from the previous version of Kaspersky Security Center Web Console are saved.

► *To upgrade Kaspersky Security Center Web Console from version 9.0 to version 10,*

run setup.exe for version 10.

The **Kaspersky Security Center 10 Web Console Setup Wizard** window opens. Follow the instructions of the Wizard.

We recommend that you avoid aborting the Setup Wizard operation.
Aborting the upgrading process at the stage of Kaspersky Security Center 10 Web Console installation may lead to the inoperability of Kaspersky Security Center Web Console 9.0.

Advanced configuration of Kaspersky Security Center 10 Web Console and Self Service Portal

After you install Kaspersky Security Center 10 Web Console and Self Service Portal, you can perform advanced configuration for them:

- Create files with the text of the End User License Agreement and FAQ that users can view when accessing Kaspersky Security Center 10 Web Console and Self Service Portal (see section "Configuring the License Agreement file and the FAQ file" on page 90).
- Add your organization's logo to the interface of Kaspersky Security Center 10 Web Console and Self Service Portal (see section "Configuring a logo" on page 90).

Changing the port number for device connection

► *To change the number of port 8080 for device connection to Kaspersky Security Center 10 Web Console:*

1. Open file httpd.conf stored in the Apache Server workfolder.

   For example, <Disk>:\Program Files (x86)\KSC Apache 2.4\Apache2.4\conf\httpd.conf".

2. Replace 8080 with the required port value in three fragments:

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

3. Restart the Apache Server service.

4. Restart Kaspersky Security Center 10 Web Console.

Example:

If you need to replace 8080 with 443, the result must be as follows:

String 1: `Listen 443`

String 38: `<VirtualHost *:443>`

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

► *To change the number of port 8081 for device connection to Self Service Portal:*

1. Open file httpd.conf stored in the Apache Server workfolder.

   For example, <Disk>:\Program Files (x86)\KSC Apache 2.4\Apache2.4\conf\httpd.conf" with notepad++

2. Replace 8081 with the required port value in three fragments:

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

3. Restart the Apache Server service.

4. Restart Self Service Portal.

We recommend that you avoid using port 80 for device connection to Kaspersky Security Center 10 Web Console or Self Service Portal, because port 80 is the port assigned to HTTP by default, while device connection to Kaspersky Security Center 10 Web Console and Self Service Portal is performed through HTTPS.

Configuring a License Agreement file and an FAQ file

► *To make available the text of the End User License Agreement and the answers to frequently asked questions through the Kaspersky Security Center 10 Web Console interface and / or through the Self Service Portal interface:*

1. Create a License Agreement file (eula.txt or eula.html) and a file with answers to frequently asked questions (FAQ) (faq.txt or faq.html).
2. Copy the created files to the installation folder of Apache Server, into a nested folder named htdocs\help.

The text of the End User License Agreement and the answers to frequently asked questions are available by clicking the respective links in the main window of Kaspersky Security Center 10 Web Console and/or in the main window of Self Service Portal.

Configuring a logo

► *To enable the display of your organization's logo in the Kaspersky Security Center 10 Web Console interface and/or in the Self Service Portal interface:*

1. Prepare a logo file meeting the following requirements:
   - file format: PNG;
   - file name: logo.png;
   - Logo size: 220×72 pixels.
2. Place the logo file to the installation folder of the Apache server:
   - If the Apache server is installed under Microsoft Windows, the path to the default installation folder is as follows: C:\Program Files\Apache Software Foundation\Apache2.2\htdocs\images\custom_logo.
   - If the Apache server is installed under Linux, the path to the default installation folder is as follows: /opt/kaspersky/kscwebconsole/share/htdocs/images/custom_logo.

Configuring a protection system for a client organization's network

This section describes the specifics of configuring a protection system using Administration Console in a client organization's network.

Protection system configuration makes part of the process of protection deployment on a client organization's network. The procedure of protection system configuration comprises the following steps:

1. Selecting the device, which will act as update agent in the client organization’s network.
2. Local installation of Network Agent on a device selected to act as update agent.
3. Remote installation of Network Agent and required Kaspersky Lab applications on the client organization’s devices.

   > This section describes the prerequisites for remote installation of applications on devices of a client organization. The procedure of remote installation of Network Agent and Kaspersky Lab anti-virus applications is described in details in the Remote installation of applications section (see page 97).

4. Creating a hierarchy of administration groups subordinate to the virtual Administration Server.

In this section:

Assigning a device to act as update agent. Configuring an update agent 92

Local installation of Network Agent on a device selected to act as update agent 93

Prerequisites for installing applications on devices of a client organization 95

Creating a hierarchy of administration groups subordinate to the virtual Administration Server 96

Assigning a device to act as update agent. Configuring an update agent

You can use a connection gateway to manage devices in a client organization when they have no direct connection with the virtual Administration Server.

You can also manually assign a device to act as update agent for an administration group and configure it as connection gateway in Administration Console.

► *To define a device as update agent of an administration group:*

1. In the console tree, select the Administration Server node.
2. In the context menu of the Administration Server, select **Properties**.
3. In the Administration Server properties window, select the **Update agents** section and click the **Add** button.

   This opens the **Add update agent** window.
4. In the **Add update agent** window, perform the following actions:

   a. Select the device that will act as update agent by clicking  on the right of the **Add** button. You can add the device in any of the following ways:

   - **Add device from group**. Adds a device from the **Managed devices** folder.
   - **Add connection gateway in DMZ by address**. Prompts you to enter the connection gateway address.

   You can use this option only for adding a Firewall-protected device as update agent, since it cannot be included in an administration group directly.

   When selecting a device, keep in mind the operation features of update agents and requirements set for the device that acts as update agent.

   b. Indicate the specific devices to which the update agent will distribute updates. You can specify an administration group or a Network Location Awareness (NLA) subnet.
5. Click the OK button.

The update agent that you have added will be displayed in the list of update agents, in the Update agents section.

> The first device with Network Agent installed that connects to the virtual Administration Server will be automatically assigned to act as update agent and configured as connection gateway.

After the update agent is added by IP address, the Administration Server will detect it next time it scans the network, moving it to the **Unassigned devices** folder. Because the update agent is protected by Firewall, you should perform the following actions to configure it.

1. Add this device to the selected administration group.
2. Reopen the Administration Server properties window on the **Update agents** section.
3. Remove the device that was added by address from the list of update agents.
4. Add the same device from the **Managed devices** folder by using the **Add** or **Add device from group** button.
5. In the properties window of this update agent in the **Advanced** section check whether the **Connection gateway** and **Initiate gateway connection from Administration Server part** check boxes are selected.

Local installation of Network Agent on a device selected to act as update agent

To allow the device assigned to act as update agent to connect to the virtual Administration Server directly and then act as connection gateway, Network Agent must be installed locally on that device.

The procedure of local installation of Network Agent on a device assigned to act as update agent is identical to local installation of Network Agent on any networked device.

The following conditions must be met by a device assigned to act as update agent:

- During local installation of Network Agent, in the **Administration Server** window of the Setup Wizard, in the **Server Address** field, specify the address of the virtual Administration Server that manages the device. You can use either the device IP address or device name in the Windows network.

  The following structure is used for the virtual Server address: **<Full address of the physical Administration Server to which the virtual Server belongs>/<Name of virtual Administration Server>**.

- To use the device as a connection gateway, open all of its ports that are required for connection with the Administration Server.

After Network Agent with the specified settings is installed on the device, Kaspersky Security Center performs the following actions automatically:

- Includes this device in the **Managed devices** group of the virtual Administration Server.
- Assigns this device to act as the update agent of the **Managed devices** group of the virtual Administration Server.

> It is necessary and sufficient to perform local installation of Network Agent on the device assigned to act as the update agent for the **Managed devices** group in the corporate network. You can install Network Agent remotely on devices that act as update agents in the nested administration groups. To do this, use the update agent of the **Managed devices** group as connection gateway.

See also:

Local installation of Network Agent 125

Remote installation of applications 97

Prerequisites for installing applications on devices of a client organization

Remote installation of applications on devices of a client organization is identical to that within an enterprise (see section "Remote installation of software" (see page 97)).

To install applications on devices of a client organization, the following conditions must be met:

- Before installing applications on devices of the client organization for the first time, you have to install Network Agent on them.

  When configuring the Network Agent installation package on the service provider side in Kaspersky Security Center, you should adjust the following settings in the properties window of the installation package.

  - In the **Connection** section, the **Server address** string, specify the address of the same virtual Administration Server that was specified during local installation of Network Agent on the update agent.
  - In the **Advanced** section, select the **Connect to Administration Server using connection gateway** check box. In the **Connection gateway address** string, specify the update agent address. You can use either the device IP address or device name in the Windows network.

- Select **Using operating system resources by means of update agents** as the download mode for the Network Agent installation package. You can select the download mode in this way:

  - If you install application by using remote installation task, you can specify the download mode in two ways:
    - when creating a remote installation task in the **Settings** window;
    - in remote installation task properties window, the **Settings** section
  - If you install applications using Remote Installation Wizard, you can select the download mode in the **Settings** window of this wizard.

- The account used by the update agent for authorization must have access to the Admin$ resource on all client devices.

Creating a hierarchy of administration groups subordinate to the virtual Administration Server

After the virtual Administration Server is created, it contains by default an administration group named **Managed devices**.

The procedure for creating a hierarchy of administration groups subordinate to a virtual Administration Server is the same as the procedure for creating a hierarchy of administration groups subordinate to the physical Administration Server. This procedure is given in the *Kaspersky Security Center Administrator's Guide*.

> You cannot add slave and virtual Administration Servers to administration groups subordinate to a virtual Administration Server. This is due to the virtual Administration Server restrictions described in *Kaspersky Security Center Administrator's Guide*.

Remote installation of applications

This section describes the methods for remote installation of Kaspersky Lab applications and their removal from networked devices.

> Before installing applications on client devices, make sure that the hardware and software of those devices meets the respective requirements.

This section describes remote installation of applications through the Administration Console.

Network Agent provides connection between the Administration Server and client devices. Network Agent must be, therefore, installed on each client device, which is to be connected to the remote centralized control system.

> The device with Administration Server installed can only use the server version of Network Agent. It is included in Administration Server as a part that is installed and removed together with it. You do not have to install Network Agent on that device.

Network Agent can be installed remotely or locally like any application. During centralized installation of security applications through Administration Console, you can install Network Agent together with those security applications.

Network Agents can differ depending upon the Kaspersky Lab applications that they are installed to support and control. In some cases Network Agent can be installed locally only (for details please refer to the documentation for the corresponding applications). Network Agent is installed on a client device only once.

Kaspersky Lab applications are managed through the Administration Console by using management plug-ins. Therefore, to access the application management interface through Kaspersky Security Center, the corresponding management plug-in must be installed on the administrator's workstation.

You can perform remote installation of applications from the administrator's workstation in the main window of the Kaspersky Security Center application.

Some Kaspersky Lab applications can be installed on client devices only locally (for details refer to the Guides of the corresponding applications). However, remote management through Kaspersky Security Center will be available for those applications.

To install software remotely, you must create a remote installation task:

The created task for remote installation will start in accordance with its schedule. You can interrupt the installation procedure by stopping the task manually.

If remote installation of an application returns an error, you can find the cause and fix it through the remote deployment preparation utility (see section "Preparing a device for remote installation). Utility tool riprep.exe" on page 118).

You can monitor the progress of remote installation of Kaspersky Lab security applications in the network using the deployment report.

Kaspersky Security Center supports remote management of the following Kaspersky Lab applications:

- For workstations:
  - Kaspersky Endpoint Security 10 for Windows (all versions supported).
  - Kaspersky Endpoint Security 8 for Linux (all versions supported).
  - Kaspersky Endpoint Security 10 for Linux (scheduled for release in 2016, 2nd half).
  - Kaspersky Endpoint Security 8 for Mac (all versions supported).
  - Kaspersky Endpoint Security 10 for Mac (scheduled for release in 2016, 2nd half).
  - Kaspersky Embedded Systems Security for Windows (scheduled for release in 2016, November).
- For mobile devices:
  - Kaspersky Security 10 for Mobile (installation available after activation of Mobile Device Management feature)

- For file servers:
  - Kaspersky Endpoint Security 10 for Windows (all versions supported).
  - Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition (all versions supported).
  - Kaspersky Security 10 for Windows Server (scheduled for release in 2016, 2nd half).
  - Kaspersky Anti-Virus 8.0 for Linux File Server (all versions supported).
  - Kaspersky Anti-Virus 10 for Linux File Server (scheduled for release in 2016, 2nd half).
- For virtual machines:
  - Kaspersky Security for Virtualization 3.0 Agentless.
  - Kaspersky Security for Virtualization 3.0. Light Agent (all versions supported).
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Nodes.

You can obtain information about the latest versions of software from the Technical Support Service website on the application page of Kaspersky Security Center in the General Info section (http://support.kaspersky.com/12029).

For details about management of the listed applications in Kaspersky Security Center, please refer to the documentation for the corresponding applications.

In this section:

Installing applications using a remote installation task 100

Installing applications using Remote Installation Wizard 106

Viewing a protection deployment report 107

Remote removal of applications 108

Work with installation packages 111

Retrieving up-to-date versions of applications 116

Preparing a device for remote installation. Utility tool riprep.exe 118

Installing applications using a remote installation task

Kaspersky Security Center allows you to install applications on devices remotely, using remote installation tasks. Those tasks are created and assigned to devices through a dedicated Wizard. To assign a task to devices more quickly and easily, you can specify devices in the Wizard window in any convenient way:

- **Select networked devices discovered by Administration Server**. In this case, the task is assigned to specific devices. Your set of specific devices can include both devices in administration groups and unassigned ones.
- **Specify device addresses manually, or import addresses from list**. You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you need to assign the task.
- **Assign task to a device selection**. In this case, the task is assigned to devices included in a previously created selection. You can specify the default selection or a custom one that you created.
- **Assign task to an administration group**. In this case, the task is assigned to devices included in a previously created administration group.

For correct remote installation on a device with no Network Agent installed, the following ports must be opened: a) TCP 139 and 445; b) UDP 137 and 138. By default, these ports are opened on all devices included in the domain. They can be opened automatically through the remote installation preparation utility (see section "Preparing a device for remote installation. Utility tool riprep.exe" on page 118).

In this section:

Installing an application on selected devices 101

Installing an application on client devices in an administration group 102

Installing an application through Active Directory group policies 102

Installing applications on slave Administration Servers 105

Installing an application on selected devices

► *To install an application on selected devices:*

1. Establish connection with the Administration Server that controls the relevant devices.
2. In the console tree, select the **Tasks** folder.
3. Run the task creation by clicking the **Create a task** link.

   This starts the New Task Wizard. Follow the instructions of the Wizard.

   In the **Task type** window of the New Task Wizard in the **Kaspersky Security Center Administration Server** section, select the **Install application remotely** task.

   The New Task Wizard creates a task of remote installation of the selected application on specific devices. The newly created task is displayed in the workspace of the **Tasks** folder.

4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

On completion of the remote installation task, the selected application will be installed on the selected devices.

Installing an application on client devices in an administration group

► *To install an application on client devices in an administration group:*

1. Establish a connection with the Administration Server that controls the relevant administration group.

2. Select an administration group in the console tree.

3. In the group workspace, open the **Tasks** tab.

4. Run the task creation by clicking the **Create a task** link.

   This starts the New Task Wizard. Follow the instructions of the Wizard.

   In the **Task type** window of the New Task Wizard in the **Kaspersky Security Center Administration Server** section, select the **Install application remotely** task.

   The New Task Wizard creates a group task of remote installation of the selected application. The new task appears in the workspace of the administration group on the **Tasks** tab.

5. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

When the remote installation task is performed, the selected application is installed on all client devices in the administration group.

Installing an application using Active Directory group policies

Kaspersky Security Center allows you to install Kaspersky Lab applications by using Active Directory group policies.

> You can install applications using Active Directory group policies only by using installation packages that include Network Agent.

► *To install an application using Active Directory group policies:*

1. Run the creation of a group remote installation task or a remote installation task for specific devices.

2. In the New Task Wizard's **Settings** window select the **Assign the package installation in the Active Directory group policies** check box.

3. Run the created remote installation task manually or wait for its scheduled start.

This starts the following remote installation sequence:

1. When the task is running, the following objects are created in each domain that includes any client devices from the specified set:

   - A group policy under the name **Kaspersky_AK{GUID}**

   - the **Kaspersky_AK{GUID}** security group that corresponds to the group policy. This security group includes client devices covered by the task. The content of the security group defines the scope of the group policy.

2. In this case, applications are installed on client devices directly from **Share**, i.e., the shared network folder of the application. In the Kaspersky Security Center installation folder, an auxiliary nested folder will be created that contains the .msi file for the application to be installed.

3. When new devices are added to the task scope, they are added to the security group after the next task start. If the **Run missed tasks** check box is selected in the task schedule, devices are added to the security group immediately.

4. When devices are deleted from the task scope, they are deleted from the security group after the next task start.

5. When a task is deleted from Active Directory, the policy, the link to the policy, and the corresponding security group are deleted.

If you want to apply another installation scheme using Active Directory, you can configure the required settings manually. This may be required in the following cases, for example:

- when the anti-virus protection administrator does not have rights to make changes to the Active Directory of certain domains;

- when the original installation package needs to be stored on a separate network resource;

- when it is necessary to link a group policy to specific Active Directory units.

The following options for using an alternative installation scheme through Active Directory are available:

- If installation is to be performed directly from the Kaspersky Security Center shared folder, in the Active Directory group policy properties you must specify the .msi file located in the exec subfolder of the installation package folder for the required application.

- If the installation package has to be located on another network resource, you must copy the whole exec folder content to it, because in addition to the file with .msi extension the folder contains configuration files generated when the package was created. To install the key with the application, copy the key file to this folder as well.

Installing applications on slave Administration Servers

► *To install an application on slave Administration Servers:*

1. Establish a connection with the Administration Server that controls the relevant slave Administration Servers.

2. Make sure that the installation package corresponding to the application being installed is available on each one of the selected slave Administration Servers. If the installation package cannot be found on any of the slave Servers, distribute it by using the installation package distribution task (see section "Distributing installation packages to slave Administration Servers" on page 113).

3. Start the creation of the task of application installation on slave Administration Servers in one of the following ways:

   - If you need to create the task for slave Administration Servers of a selected administration group, run creation of a group task of remote installation for that group (see section "Installing an application on client devices in an administration group" on page 102).

   - If you need to create a task for specific slave Administration Servers, run creation of a remote installation task for specific devices (see section "Installing an application on selected devices" on page 101).

   This starts the Deployment Task Creation Wizard creating the remote installation task. Follow the instructions of the Wizard.

   In the **Task type** window of the New Task Wizard, in the **Kaspersky Security Center Administration Server** section, open the **Advanced** folder and select the task named **Install application on slave Administration Servers remotely**.

   The New Task Wizard will create the task of remote installation of the selected application on specific slave Administration Servers.

4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

On completion of the remote installation task, the selected application will be installed on slave Administration Servers.

Installing applications using Remote Installation Wizard

To install Kaspersky Lab applications, you can use the Remote Installation Wizard. The Remote Installation Wizard allows remote installation of applications either through pre-created installation packages or directly from a distribution package.

For the proper operation of the remote installation task on a client device with no Network Agent installed, the following ports must be open: TCP 139 and 445; UDP 137 and 138. By default, these ports are open for all devices included in the domain. They can be opened automatically through the remote installation preparation utility (see section "Preparing a device for remote installation. Utility tool riprep.exe" on page 118).

► *To install the application using the Remote Installation Wizard:*

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the workspace of the group, click the **Perform action** button and select **Install application** in the drop-down list.

   This will start the Remote Installation Wizard. Follow the instructions of the Wizard.
4. At the final step of the Wizard, click **Next** to create and run a remote installation task on the selected devices.

When the Remote Installation Wizard completes, Kaspersky Security Center performs the following actions:

- Creates an installation package for application installation (if it was not created earlier). The installation package is located in the **Remote installation** folder, in the **Installation packages** subfolder, under a name that corresponds to the application's name and version. You can use this installation package for the application installation in the future.
- It creates and runs a remote installation task for specific devices or for an administration group. The newly created remote installation task is stored in the **Tasks** folder or added to the tasks of the administration group for which it has been created. You can later launch this task manually. The task name corresponds to the name of the application installation package: **Installation <Name of installation package>**.

Viewing a protection deployment report

You can use the protection deployment report to monitor the progress of network protection deployment.

► *To view a protection deployment report:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Reports** tab.
3. In the workspace of the **Reports** folder, select the report template named **Protection deployment report**.

The workspace displays a report containing information about protection deployment on all networked devices.

You can generate a new protection deployment report and specify the type of data that it should include:

- For an administration group.
- For specific devices.

- For a device selection.
- For all devices.

For detailed information about how to create a new report refer to the *Administrator's Guide of Kaspersky Security Center*.

Kaspersky Security Center assumes that a device has protection deployed if it has a security application installed and real-time protection enabled.

Remote removal of applications

Kaspersky Security Center allows you to uninstall applications from devices remotely through remote uninstallation tasks. Those tasks are created and assigned to devices through a dedicated Wizard. To assign a task to devices more quickly and easily, you can specify devices in the Wizard window in any convenient way:

- **Select networked devices discovered by Administration Server**. In this case, the task is assigned to specific devices. Your set of specific devices can include both devices in administration groups and unassigned ones.
- **Specify device addresses manually, or import addresses from list**. You can specify NetBIOS names, DNS names, IP addresses, and IP subnets of devices to which you need to assign the task.
- **Assign task to a device selection**. In this case, the task is assigned to devices included in a previously created selection. You can specify the default selection or a custom one that you created.
- **Assign task to an administration group**. In this case, the task is assigned to devices included in a previously created administration group.

In this section:

Remote removal of an application from client devices of an administration group 109

Remote removal of an application from selected devices 110

Remote removal of an application from client devices of an administration group

► *To remove an application remotely from client devices of an administration group:*

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the group workspace, open the **Tasks** tab.
4. Run the task creation by clicking the **Create a task** link.

   This starts the New Task Wizard. Follow the instructions of the Wizard.

   In the **Task type** window of the New Task Wizard, in the **Kaspersky Security Center Administration Server** node, in the **Advanced** folder select the **Uninstall application remotely** task.

   The New Task Wizard creates a group task of remote removal of the selected application. The new task appears in the workspace of the administration group on the **Tasks** tab.
5. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

Once the remote removal task is complete, the selected application is removed from client devices of this administration group.

Remote removal of an application from selected devices

► *To remove an application remotely from selected devices:*

1. Establish connection with the Administration Server that controls the relevant devices.
2. In the console tree, select the **Tasks** folder.

3. Run task creation by clicking **Create a Task**.

   This starts the New Task Wizard. Follow the instructions of the Wizard.

   In the **Task type** window of the New Task Wizard, in the **Kaspersky Security Center Administration Server** node, in the **Advanced** folder select the **Uninstall application remotely** task.

   The New Task Wizard creates a task of remote removal of the selected application from specific devices. The newly created task is displayed in the workspace of the **Tasks** folder.

4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

Upon completion of the remote removal task, the selected application will be removed from the selected devices.

Work with installation packages

When creating remote installation tasks the system uses installation packages containing sets of parameters necessary for software installation.

> Installation packages can contain a key file. We recommend that you avoid sharing access to installation packages that contain a key file.

You can use a single installation package several times.

Installation packages created for Administration Server are moved to the console tree and located in the **Remote installation** folder, in the **Installation packages** subfolder. Installation packages are stored on the Administration Server, in a service subfolder named Packages, within the specified shared folder.

In this section:

Creating an installation package 112

Distributing installation packages to slave Administration Servers 113

Distributing installation packages through update agents 114

Transferring application installation results to Kaspersky Security Center 114

Creating an installation package

► *To create an installation package, do the following:*

1. Connect to the necessary Administration Server.
2. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
3. Launch the process of installation package creation in one of the following ways:
   - from the context menu of the **Installation packages** folder select **Create** → **Installation package**;
   - in the context menu of the list of installation packages, select **Create** → **Installation package**;
   - click the **Create installation package** link in the installation package control section.

This will start the New Package Wizard. Follow the instructions of the Wizard.

When creating an installation package for the Kaspersky Lab application, you may be prompted to view the License Agreement for this application. Read the License Agreement through carefully! If you agree with all of its terms, select the **I accept the terms of the License Agreement** check box. After that, creation of the installation package continues. The path to the License Agreement file is specified in a KUD or KPD file included in the distribution kit of the application for which the installation package is to be created.

> When you create an installation package for Kaspersky Endpoint Security for Mac, you can select the language of the End User License Agreement.

When creating an installation package for an application from the Kaspersky Lab database of applications, you can enable automatic installation of system components (prerequisites) required for installation of the application. The New Package Wizard displays a list of all available system components for the selected application. When creating a patch installation package (incomplete distribution package), the list contains all system prerequisites for deployment of the patch, up to the full distribution package. You can find that list at any time in installation package properties.

After completion of the New Package Wizard sequence, the new installation package appears in the workspace of the **Installation packages** folder.

There is no need to manually create an installation package for remote installation of Network Agent. It is created automatically during Kaspersky Security Center installation and is stored in the **Installation packages** folder. If the package for remote installation of the Network Agent has been deleted, to re-create it you select the nagent10.kud file in the NetAgent folder of the Kaspersky Security Center distribution package.

Do not specify any details of privileged user accounts in the settings of installation packages.

When an installation package for Administration Server is created, select the sc10.kud file in the root folder of the Kaspersky Security Center distribution package as the description file.

Distributing installation packages to slave Administration Servers

► *To distribute installation packages to slave Administration Servers:*

1. Establish a connection with the Administration Server that controls the relevant slave Administration Servers.
2. Start the creation of a task of installation package distribution to slave Administration Servers in one of the following ways:
   - If you want to create a task for slave Administration Servers in the selected administration group, launch the creation of a group task for this group.
   - If you want to create a task for specific slave Administration Serves, run creation of a task for specific devices.

   This starts the New Task Wizard. Follow the instructions of the Wizard.

   In the **Task type** window of the New Task Wizard, in the **Kaspersky Security Center Administration Server** node, open the **Advanced** folder and select the task type named **Distribute installation package**.

   The New Task Wizard will create the task of distributing the selected installation packages to specific slave Administration Servers.

3. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

As a result of this task, the selected installation packages will be copied to the specific slave Administration Servers.

Distributing installation packages through update agents

You can use update agents to distribute installation packages within an administration group.

After the installation packages are received from the Administration Server, update agents automatically distribute them to client devices through IP multicasting. New installation packages are distributed within an administration group once. If a client device has been disconnected from the corporate network during the distribution session, Network Agent installed on that client device automatically downloads the relevant installation package from the update agent when the installation task is started.

Transferring application installation results to Kaspersky Security Center

After you have created the application installation package, you can configure it so that all diagnostic information about the results of the application installation is transferred to Kaspersky Security Center. For installation packages of Kaspersky Lab applications, transfer of diagnostic information about the application installation results is configured by default, no additional configuration is required.

► *To configure the transfer of diagnostic information about the results of application installation to Kaspersky Security Center:*

1. Navigate to the folder of the installation package created by using Kaspersky Security Center for the selected application. The folder can be found in the shared folder specified during Kaspersky Security Center installation.

2. Open the file with the .kpd or .kud extension for editing (for example, in the Microsoft Windows Notepad editor).

The file has the format of a regular configuration .ini file.

3. Add the following lines to the file:

   ```
   [SetupProcessResult]

   Wait=1
   ```

   This command configures Kaspersky Security Center to wait for setup completion for the application, for which the installation package is created, and to analyze the installer return code. If you have to disable the transfer of diagnostic data, set the Wait key to 0.

4. Add the description of return codes for a successful installation. To do this, add the following lines to the file:

   ```
   [SetupProcessResult_SuccessCodes]

   <return code>=[<description>]

   <return code 1>=[<description>]

     …
   ```

   > Square brackets contain optional keys.

   Syntax for the lines:

   - `<return code>`. Any number corresponding to the installer return code. The number of return codes can be arbitrary.
   - `<description>`. Text description of the installation result. The description can be omitted.

5. Add the description of return codes for a failed installation. To do this, add the following lines to the file:

   ```
   [SetupProcessResult_ErrorCodes]

   <return code>=[<description>]

   <return code 1>=[<description>]

   …
   ```

   The syntax of these lines is identical to the syntax for the lines containing successful setup return codes.

6. Close the .kpd or .kud file by saving all changes.

Finally, the results of installation of the user-defined application will be registered in the logs of Kaspersky Security Center and then shown in the list of events, in reports, and in task run logs.

Retrieving up-to-date versions of applications

Kaspersky Security Center allows retrieving up-to-date versions of corporate applications stored on Kaspersky Lab servers.

► *To retrieve up-to-date versions of corporate applications by Kaspersky Lab:*

1. Open the main window of Kaspersky Security Center.
2. Open the **Current application versions** window by clicking the **There are new versions of Kaspersky Lab products available** link in the **Deployment** section.

   The **There are new versions of Kaspersky Lab products available** link becomes available when Administration Server finds a new version of a corporate application on a Kaspersky Lab server.

3. Select the required application from the list.
4. Download the application distribution package by clicking the link in the **Distribution package web address** string.

   If the **Download applications and create installation packages** button is displayed for the application selected, you can click this button to download the application distribution package and create an installation package automatically. As a result, Kaspersky Security Center downloads the application distribution package to Administration Server, to the shared folder specified when installing Kaspersky Security Center. The automatically created installation package is displayed in the **Remote installation** folder of the console tree, in the **Installation packages** subfolder.

After the **Current application versions** window is closed, the **There are new versions of Kaspersky Lab products available** link disappears from the **Deployment** section.

You can create installation packages for new versions of applications and manage newly created installation packages in the **Remote installation** folder of the console tree, in the **Installation packages** subfolder.

You can also open the **Current application versions** window by clicking the **View current version of Kaspersky Lab applications** link in the workspace of the **Installation packages** folder.

See also:

Installing applications using a remote installation task 100

Installing applications using Remote Installation Wizard 106

Viewing a protection deployment report 107

Remote removal of applications 108

Work with installation packages 111

Preparing a device for remote installation. Utility tool riprep.exe 118

Creating an installation package 112

Preparing a device for remote installation. Utility tool riprep.exe

Remote installation of an application on a client device may return an error for the following reasons:

- The task has already been successfully performed on this device. In this case, the task does not have to be performed again.
- When the task was started, the device was shut down. In this case, turn on the device and start the task again.
- There is no connection between the Administration Server and Network Agent installed on the client device. To find the cause of this problem, use the utility designed for remote diagnostics on devices (klactgui). For detailed information about how to use this utility refer to the *Administrator's Guide of Kaspersky Security Center*.
- If no Network Agent is installed on the device, the following problems may occur during remote installation:
  - The client device has the **Simple file sharing** setting enabled.
  - The Server service is not running on the client device.
  - The relevant ports are closed on the client device.
  - The user account that is used to perform the task has insufficient privileges.

  To solve problems that have occurred during the application installation on a client device without Network Agent installed, you can use the utility designed for preparation of devices for remote installation (riprep).

This section describes the utility, which allows you to prepare a device for remote installation (riprep). The utility is located in the Kaspersky Security Center installation folder on the device with Administration Server installed.

The utility used to prepare a device for remote installation cannot run under Microsoft Windows XP Home Edition.

In this section:

Preparing a device for remote installation in interactive mode 119

Preparing a device for remote installation in non-interactive mode 121

Preparing a device for remote installation in interactive mode

► *To prepare a device for remote installation in interactive mode:*

1. Run the riprep.exe file on the client device.
2. In the main window of the remote installation preparation utility that opens, select the following check boxes:
   - **Disable simple file sharing**.
   - **Start the Server service**.
   - **Open ports**.
   - **Add an account**.
   - **Disable User Account Control (UAC)**. This setting is only available for computers running under Microsoft Windows Vista, Microsoft Windows 7, or Microsoft Windows Server 2008.
3. Click the **Start** button.

   As a result, the stages of device preparation for remote installation are displayed in the lower part of the utility's main window.

If you have selected the **Add an account** check box, a request to enter the account name and password will be displayed when an account is created. This will create a local account, which belongs to the local administrators' group.

If you select the **Disable User Account Control (UAC)** check box, an attempt to disable User Account Control will be made even if UAC was disabled before the utility was started. After you disable UAC, you are prompted to restart the device.

Preparing a device for remote installation in non-interactive mode

► *To prepare a device for remote installation in silent mode:*

run the riprep.exe file on the client device from the command line with the relevant set of keys.

Utility command line syntax:

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

The command-line parameters are as follows:

- `-silent` – Starts the utility in the non-interactive mode.
- `-cfg CONFIG_FILE` – Defines the utility configuration, where `CONFIG_FILE` is the path to the configuration file (a file with the .ini extension).
- `-tl traceLevel` – Defines the trace level, where `traceLevel` is a number from 0 to 5. If no key is specified, the value 0 is used.

You can perform the following tasks by starting the utility in silent mode:

- Disabling the simple sharing of files
- Starting the Server service on the client device
- Opening the ports
- Creating a local account
- Disabling User Account Control (UAC)

You can define the settings of device preparation for remote installation in the configuration file specified in the `-cfg` key. To define these settings, add the following information to the configuration file:

- In the `Common` section, specify the tasks to be performed:
  - `DisableSFS` – Disable simple file sharing (0 – the task is disabled; 1 – the task is enabled).
  - `StartServer` – Start the Server service (0 – the task is disabled; 1 – the task is enabled).

- `OpenFirewallPorts` – Open the necessary ports (0 – the task is disabled; 1 – the task is enabled).
- `DisableUAC` – Disable User Account Control (0 – the task is disabled; 1 – the task is enabled).
- `RebootType`– Define behavior if restart of computer is required when UAC is disabled. You can use the following values:
  - 0—Never restart the device.
  - 1—Restart the device if UAC had been enabled before the utility was started.
  - 2—Force the restart if UAC had been enabled before the utility was started.
  - 4—Always restart the device.
  - 5—Always force the device to restart.

- In the `UserAccount` section, specify the account name (`user`) and its password (`Pwd`).

Sample context of the configuration file:

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

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

After the utility completes, the following files will be created in the utility start folder:

- riprep.txt– Operation report, in which phases of the utility operation are listed with reasons for these operations.
- riprep.log – The trace file (created if the tracing level is set above 0).

Local installation of applications

This section provides the installation procedure for applications that can only be installed on a local device.

To perform local installation of applications on a selected client device, you must have administrator rights on that device.

► *To install applications locally on a selected client device:*

1. Install Network Agent on the client device and set up connection between the client device and the Administration Server.
2. Install the relevant applications on the device as described in the Guides of these applications.
3. Install a management plug-in for each of the installed applications on the administrator's workstation.

Kaspersky Security Center also supports the option of local installation of applications using a stand-alone installation package.

Creation of stand-alone installation packages is only available for the following applications:

- For workstations:
  - Kaspersky Endpoint Security 10 for Windows (all versions supported).
  - Kaspersky Endpoint Security 10 for Linux (scheduled for release in 2016, 2nd half).
  - Kaspersky Endpoint Security 8 for Linux (all versions supported).
  - Kaspersky Endpoint Security 10 for Mac (scheduled for release in 2016, 2nd half).
  - Kaspersky Endpoint Security 8 for Mac (all versions supported).
  - Kaspersky Embedded Systems Security for Windows (scheduled for release in 2016, November).

- For mobile devices:
  - Kaspersky Security 10 for Mobile (installation available after activation of Mobile Device Management feature).
- For mail systems and sharepoint / collaboration servers:
  - Kaspersky Security 8.0 for Linux Mail Server Maintenance Pack 1 (or later).
  - Kaspersky Secure Mail Gateway 1.0.
  - Kaspersky Security for Microsoft Exchange Servers (scheduled for release in 2016, 2nd half).
  - Kaspersky Security for SharePoint Server (scheduled for release in 2016, 2nd half).
- For file servers:
  - Kaspersky Endpoint Security 10 for Windows (all versions supported).
  - Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition (all versions supported).
  - Kaspersky Security 10 for Windows Server (scheduled for release in 2016, 2nd half).
  - Kaspersky Anti-Virus 8.0 for Linux File Server (all versions supported).
  - Kaspersky Anti-Virus 10 for Linux File Server (scheduled for release in 2016, 2nd half).
- For virtual machines:
  - Kaspersky Security for Virtualization 3.0 Agentless.
  - Kaspersky Security for Virtualization 4.0 Agentless (scheduled for release in 2016, November).
  - Kaspersky Security for Virtualization 3.0 Light Agent (all versions supported).
  - Kaspersky Security for Virtualization 4.0 Light Agent (scheduled for release in 2016, November).
- Kaspersky Industrial Cyber Security:
  - Kaspersky Industrial Cyber Security for Networks.
  - Kaspersky Industrial Cyber Security for Nodes.

You can obtain information about the latest versions of software from the Technical Support Service website on the application page of Kaspersky Security Center 10 in the General Info section (http://support.kaspersky.com/12029).

In this section:

Local installation of Network Agent 125

Installing Network Agent in non-interactive mode..... 127

Local installation of the application management plug-in..... 129

Installing applications in non-interactive mode 130

Installing software by using stand-alone packages 131

Local installation of Network Agent

► *To install Network Agent on a device locally:*

1. On the device, run the setup.exe file from the distribution CD or from the distribution package downloaded from the Internet.

   A window opens prompting you to select Kaspersky Lab applications to install.

2. In the application selection window, click **Install only Kaspersky Security Center 10 Network Agent** to run the Network Agent Setup Wizard. Follow the instructions of the Wizard.

   While the Installation Wizard is running, you can define the advanced settings of Network Agent (see below). The installation of Network Agent from the distribution package downloaded from the Internet does not differ from the installation from the installation CD.

3. If you want to use your device as the connection gateway for a specific administration group, in the **Connection gateway** window of the Setup Wizard, select **Use as connection gateway in DMZ**.

4. To configure Network Agent during installation on a virtual machine:

    a. Enable the dynamic mode of Network Agent for Virtual Desktop Infrastructure (VDI). To do this, in the **Advanced Settings** window of the Setup Wizard, select the **Enable dynamic mode for VDI** check box.

    b. Optimize the Network Agent operation for VDI. To do this, in the **Advanced Settings** window of the Setup Wizard, select the **Optimize Kaspersky Security Center Network Agent settings for virtual infrastructure** check box.

    As a result, scanning of executable files for vulnerabilities at the device startup is disabled. Also, this disables the sending of information about the following objects to Administration Server:

    - Hardware registry.
    - Applications installed on the device.
    - Updates of Microsoft Windows that must be installed on the local client device.
    - Software vulnerabilities detected on the local client device.

    Furthermore, you will be able to enable the sending of this information in the Network Agent properties or in the Network Agent policy settings.

When the Setup Wizard is complete, Network Agent is installed on the device.

You can view the properties of the Kaspersky Security Center Network Agent service, start, stop, and monitor Network Agent activity by means of standard Microsoft Windows tools: Computer management\Services.

Installing Network Agent in non-interactive mode

Network Agent can be installed in non-interactive mode, i.e., without interactive input of installation settings. Non-interactive installation requires an installation MSI package of Network Agent located in the distribution package of Kaspersky Security Center, in the folder Packages\NetAgent\exec.

► *To install Network Agent on a local device in non-interactive mode,*

run the command

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

where `setup_parameters` is a list of settings and their respective values separated by a space (`PRO1=PROP1VAL PROP2=PROP2VAL`).

Names and possible values of settings that can be used when installing Network Agent in non-interactive mode are listed in the table below.

Table 8. Settings of Network Agent installation in non-interactive mode

Setting name	Setting description	Available values
INSTALLDIR	Path to the Network Agent installation folder	String value
SERVERADDRESS	Administration Server address	String value
SERVERPORT	Port number to connect to Administration Server.	Numerical value
SERVERSSLPORT	Port number to connect to Administration Server by using SSL protocol.	Numerical value
USESSL	Whether to use SSL connection	• 1 – Use • Other value or no value – Do not use

Setting name	Setting description	Available values
OPENUDPPORT	Whether to open a UDP port	• 1 – Open • Other value or no value – Do not open
UDPPORT	UDP port number	Numerical value
USEPROXY	Whether to use a proxy server	• 1 – Use • Other value or no value – Do not use
PROXYADDRESS	Proxy address	String value
PROXYPORT	Number of port for connection to Administration Server	Numerical value
PROXYLOGIN	Name of an account for connection to a proxy server	String value
PROXYPASSWORD	Password of account for connection to proxy server. Do not specify any details of privileged user accounts in the settings of installation packages.	String value
GATEWAYMODE	Connection gateway use mode:	• 0—Do not use connection gateway. • 1—Use as connection gateway the device on which Network Agent is to be installed. • 2—Connect to the Administration Server via another connection gateway.
GATEWAYADDRESS	Connection gateway address	String value

Setting name	Setting description	Available values
CERTSELECTION	Method of receiving a certificate	• GetOnFirstConnection – Receive an Administration Server certificate • GetExistent – Select an existing certificate
CERTFILE	Path to the certificate file	String value
VMVDI	Whether to enable the dynamic mode for VDI	• 1 – Enable • Other value or no value – Do not enable
LAUNCHPROGRAM	Whether to run the Network Agent service after installation completion	• 1 – Run • Other value or no value – Do not run

Remote installation of Network Agent using an installation package or local installation in non-interactive mode mean automatic acceptance of the terms of the License Agreement related to the application to be installed. You can view the License Agreement for a specific application in the distribution kit of the application or on the Kaspersky Lab Technical Support Service website.

Local installation of the application management plug-in

► *To install the application management plug-in:*

On the device with Administration Console installed, run the klcfginst.exe file, which is included in the application distribution package.

The klcfginst.exe is included in all applications that can be controlled by Kaspersky Security Center. Installation is facilitated by a wizard and requires no manual configuration of settings.

Installing applications in non-interactive mode

► *To install an application in non-interactive mode:*

1. Open the main window of Kaspersky Security Center.
2. In the **Remote installation** folder of the console tree, in the **Installation packages** subfolder select the installation package of the required application or create a new one for that application.

   The installation package will be stored on the Administration Server in the Packages service folder within the shared folder. A separate subfolder corresponds to each installation package.

3. Open the folder storing the required installation package in one of the following ways:
   - Copy the folder corresponding to the relevant installation package from the Administration Server to the client device. Open this folder on the client device.
   - From the client device, open the shared folder on the Administration Server, which corresponds to the relevant installation package.

   If the shared folder is located on a device running Microsoft Windows Vista, select the **Disabled** value for the **User Account Control: Run all administrators in Admin Approval Mode** setting (**Start** → **Control Panel** → **Administration** → **Local security policy** → **Security settings**).

4. Depending on the selected application, do the following:
   - For Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers and Kaspersky Security Center, navigate to the exec subfolder and run the executable file (the one with the .exe extension) with the /s key.
   - For other Kaspersky Lab applications run the executable file (a file with the .exe extension) with the /s key from the open folder.

   Running the executable file with the key `EULA=1` means your acceptance of the License Agreement terms. The text of the License Agreement is included in the distribution package of Kaspersky Security Center. Accepting the terms of the License Agreement is necessary for installing the application or updating a previous version of the application.

Installing software by using stand-alone packages

Kaspersky Security Center lets you create stand-alone installation packages for applications. A stand-alone installation package is an executable file that can be located on a Web Server, sent by email, or transferred to a client device in some other way. This received file can be run locally on the client device to install an application without involving Kaspersky Security Center.

► *To install an application using a stand-alone installation package:*

1. Connect to the necessary Administration Server.
2. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
3. In the workspace, select the installation package of the required application.
4. Launch the process of creating a stand-alone installation package using one of the following methods:

   - In the context menu of the installation package, select **Create stand-alone installation package**.
   - Click the **Create stand-alone installation package** link in the workspace of the installation package.

   This will start the Stand-alone Installation Package Creation Wizard. Follow the instructions of the Wizard.

   At the final step of the Wizard, select a method for transferring the stand-alone installation package to the client device.
5. Transfer the stand-alone installation package to the client device.
6. Run the stand-alone installation package on the client device.

As a result, the application is installed on the client device under the settings specified in the stand-alone package.

When you create a stand-alone installation package, it is automatically published on Web Server. The link for downloading the stand-alone package is displayed in the list of created stand-alone installation packages. You can cancel publishing of the selected stand-alone package and republish it on the Web Server. By default, port 8060 is used for downloading stand-alone installation packages.

Deploying mobile device management systems

This section describes the deployment of mobile device management systems via Exchange ActiveSync, iOS MDM, and Kaspersky Endpoint Security protocols.

In this section:

Management through iOS MDM and Microsoft Exchange ActiveSync 132

Deploying a system for management via iOS MDM protocol 136

Deploying a system for management via KES protocol using Self Service Portal 148

Adding a KES device to the list of managed devices..... 149

Management through iOS MDM and Microsoft Exchange ActiveSync

Kaspersky Security Center allows managing mobile devices that are connected to Administration Server via Exchange ActiveSync protocol. Exchange ActiveSync (EAS) mobile devices are those connected to a Microsoft Exchange Mobile Devices Server and managed by Administration Server.

The following operating systems support Exchange ActiveSync protocol:

- Windows Mobile.
- Windows CE.
- Windows Phone® 7.
- Windows Phone 8.
- Android.

- Bada.
- BlackBerry® 10.
- iOS®.
- Symbian.

> The contents of the set of management settings for an Exchange ActiveSync device depend on the operating system under which the mobile device is running. For details on the support features of Exchange ActiveSync protocol for a specific operating system, please refer to the documentation enclosed with the operating system.

Deployment of a mobile device management system using Exchange ActiveSync protocol includes the following steps:

1. The administrator installs Exchange ActiveSync Mobile Devices Server on a selected client device (see section "Installing Exchange ActiveSync Mobile Devices Server" on page 134).
2. The administrator creates a management profile(s) in Administration Console for managing EAS devices and adds that profile(s) to the mailboxes of Exchange ActiveSync users.

   > *Management profile of Exchange ActiveSync mobile devices* is an ActiveSync policy used on a Microsoft Exchange server for managing Exchange ActiveSync mobile devices. Only one EAS device management profile can be assigned to a Microsoft Exchange mailbox.

   For the instruction on how to create an EAS device management profile, please refer to the *Kaspersky Security Center Administrator's Guide*.

   Users of mobile EAS devices connect to their Exchange mailboxes. A management profile imposes restrictions on mobile devices (see section "Connecting mobile devices to Microsoft Exchange Mobile Devices Server" on page 135).

For information about how add an EAS device management profile and how to manage Exchange ActiveSync mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

Installing a Mobile device server for Exchange ActiveSync

A Microsoft Exchange Mobile Devices Server should be installed on a client device with a Microsoft Exchange server installed. It is recommended to install the Microsoft Exchange Mobile Devices Server to a Microsoft Exchange server with the Client Access role assigned. If several Microsoft Exchange servers with the Client Access role in the same domain are combined into a Client Access Array, it is recommended to install the Microsoft Exchange Mobile Devices Server on each Microsoft Exchange server in that array in cluster mode.

► *To install a Microsoft Exchange Mobile Devices Server on a local device:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

2. In the applications selection window, click the **Install Microsoft Exchange Mobile Devices Server** link to run the Microsoft Exchange Mobile Devices Server Setup Wizard.

3. Choose the type of Microsoft Exchange Mobile Devices Server installation in the **Installation settings** window:

   - To install Microsoft Exchange Mobile Devices Server with the default settings, select **Standard installation** and click the **Next** button.

   - To define the settings for installation of the Microsoft Exchange Mobile Devices Server manually, select **Advanced installation** and click **Next**. Then do the following:

     a. Select destination folder in **Destination Folder** window. The default folder is <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

     b. Choose the Microsoft Exchange Mobile Devices Server installation mode (normal or cluster) in the **Installation mode** window: normal or cluster mode.

c. In **Select Account** window, choose an account that will be used to manage mobile devices:

- **Create account and role group automatically**.
  Account will be created automatically.
- **Specify an account**. Account should be selected manually. Click the **Select** button to select the user account and specify the password. The selected user should belong to a group with rights to manage mobile devices via ActiveSync.

d. In **IIS settings** window, enable or disable automatic configuration of Internet Information Services (IIS) web server properties.

> If you have locked the automatic configuration of Internet Information Services (IIS) properties, enable the "Windows authentication" mechanism manually in IIS settings for PowerShell Virtual Directory. If "Windows authentication" mechanism is disabled, Microsoft Exchange Mobile Devices Server will not operate correctly. Please refer to IIS documentation for more information about configuring IIS.

e. Click **Next**.

4. Verify Microsoft Exchange Mobile Devices Server installation properties in the window that opens, then click **Install**.

When the Wizard is complete, the Microsoft Exchange Mobile Devices Server is installed on the local device. The Microsoft Exchange Mobile Devices Server will be displayed in the **Mobile Device Management** folder of the console tree.

Connecting mobile devices to a Microsoft Exchange Mobile Devices Server

Before connecting any mobile devices, you should configure Microsoft Exchange Server in order to allow devices to be connected via ActiveSync protocol.

To connect a mobile device to a Microsoft Exchange Mobile Devices Server, the user connects to his or her Microsoft Exchange mailbox from the mobile device through ActiveSync.

When connecting, the user must specify the connection settings in the ActiveSync client, such as email address and email password.

The user's mobile device connected to the Microsoft Exchange server is displayed in the **Mobile devices** subfolder contained in the **Mobile Device Management** folder of the console tree.

After the Exchange ActiveSync mobile device is connected to a Microsoft Exchange Mobile Devices Server, the administrator can manage the Exchange ActiveSync mobile device that has been connected. For instructions on how to manage Exchange ActiveSync mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

Deploying a system for management via iOS MDM protocol

Kaspersky Security Center allows managing mobile devices running under iOS. iOS MDM mobile devices refer to iOS mobile devices that are connected to an iOS MDM Server and managed by an Administration Server.

Connection of mobile devices to an iOS MDM Server is performed in the following sequence:

1. The administrator installs iOS MDM Server on the selected client device. Installation of iOS MDM Server is performed using the standard tools of the operating system.

2. The administrator receives an Apple® Push Notification Service certificate, also known as APNs certificate (see section "Receiving an APNs certificate" on page 143).

   The APNs certificate allows Administration Server to connect to the APNs server to send push notifications to iOS MDM mobile devices.

3. The administrator installs the APNs certificate on the iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 145).

4. The administrator creates an iOS MDM profile for the user of the iOS mobile device.

   The iOS MDM profile contains a collection of settings for connecting iOS mobile devices to Administration Server.

5. The administrator issues a shared certificate to the user (see section "Issuing and installing a shared certificate on a mobile device" on page 146).

   The shared certificate is required to confirm that the mobile device is owned by the user.

6. The user clicks the link sent by the administrator and downloads an installation package to the mobile device.

   The installation package contains a certificate and an iOS MDM profile.

   After the iOS MDM profile is downloaded and the iOS MDM mobile device is synchronized with the Administration Server, the device is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

7. The administrator adds a configuration profile on the iOS MDM Server and installs the configuration profile on the mobile device after it is connected.

   The configuration profile contains a collection of settings and restrictions for the iOS MDM mobile device, for example, settings for installation of applications, settings for the use of various features of the device, email and scheduling settings. A configuration profile lets you configure iOS MDM mobile devices in accordance with the organization's security policies.

8. If necessary, the administrator adds provisioning profiles on the iOS MDM Server and then installs these provisioning profiles on mobile devices.

   Provisioning profile is a profile that is used for managing applications distributed in ways other than via App Store®. A provisioning profile contains information about the license; it is linked to a specific application.

For instructions on how to manage iOS MDM mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

In this section:

Installing iOS MDM Server 138

Installing iOS MDM Server in non-interactive mode 140

Use of iOS MDM Server by multiple virtual Servers 142

Receiving an APNs certificate..... 143

Installing an APNs certificate on an iOS MDM Server 145

Issuing and installing a shared certificate on a mobile device 146

Adding an iOS MDM device to the list of managed devices..... 146

Installing iOS MDM Server

► *To install iOS MDM Server on a local device:*

1. Run the setup.exe executable file.

   A window opens prompting you to select Kaspersky Lab applications to install.

   In the applications selection window, click the **Install iOS MDM Server** link to run the iOS MDM Server Setup Wizard.

2. Select a destination folder.

   The default destination folder is <Disk>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.

3. In the **Settings for connection to iOS MDM Server** window of the Wizard, in the **External port to connect to iOS MDM service** field, specify an external port for connecting mobile devices to the iOS MDM service.

External port 5223 is used by mobile devices for communication with the APNs server. Make sure that port 5223 is opened in the firewall for connection with the address range 17.0.0.0/8.

Port 443 is used for connection to iOS MDM Server by default. If port 443 is already in use by another service or application, it can be replaced with, for example, port 9443.

The iOS MDM Server uses external port 2195 to send notifications to the APNs server.

APNs servers run in load balancing mode. Mobile devices do not always connect to the same IP addresses to receive notifications. The 17.0.0.0/8 address range is reserved for Apple, which is why it is recommended to specify this entire range as an allowed range in Firewall settings.

4. If you want to configure interaction ports for application components manually, select the **Set up local ports manually** check box and then specify values for the following settings:

   - **Port to connect to Network Agent**. In this field, specify a port for connecting the iOS MDM service to Network Agent. The default port number is 9799.
   - **Port for connection to iOS MDM service**. In this field, specify a local port for connecting Network Agent to the iOS MDM service. The default port number is 9899.

   It is recommended to use default values.

5. In the **External address of Mobile Device Server** window of the Wizard, in the **Web address for remote connection to Mobile Device Server** field, specify the address of the client device on which iOS MDM Server is to be installed.

   This address will be used for connecting managed mobile devices to the iOS MDM service. The client device must be available for connection of iOS MDM devices.

   You can specify the address of a client device in any of the following formats:

   - Device FQDN (such as mdm.example.com)
   - Device NetBIOS name
   - Device IP address

   Please avoid adding the URI scheme and the port number in the address string: these values will be added automatically.

When the Wizard completes, iOS MDM Server is installed on the local device. The iOS MDM Server is displayed in the **Mobile Device Management** folder of the console tree.

Installing iOS MDM Server in non-interactive mode

Kaspersky Security Center allows you to install iOS MDM Server on a local device in non-interactive mode, i.e. without interactive input of installation settings.

► *To install iOS MDM Server on a local device in non-interactive mode,*

run the command

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

where `setup_parameters` is a list of settings and their respective values separated with spaces (`PRO1=PROP1VAL PROP2=PROP2VAL`). Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center in the Server folder.

The names and possible values for settings that can be used when installing iOS MDM Server in non-interactive mode are listed in the table below. Settings can be specified in any convenient order.

Table 9. Settings of iOS MDM Server installation in non-interactive mode

Setting name	Setting description	Available values
EULA	Acceptance of the terms of the License Agreement. This setting is mandatory.	• 1 – I accept the terms of the License Agreement • Other value, or no value – I do not accept the terms of the License Agreement (installation is not performed)
DONT_USE_ANSWER_FILE	Whether or not to use an XML file with iOS MDM Server installation settings. The XML file is included in the installation package or stored on the Administration Server. You do not have to specify an additional path to the file. This setting is mandatory.	• 1 – Do not use the XML file with settings • Other value, or no value defined – use the XML file with settings

Setting name	Setting description	Available values
INSTALLDIR	iOS MDM Server installation folder. This setting is optional.	String value, for example, `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Local port for connecting the iOS MDM service to Network Agent. The default port number is 9799. This setting is optional.	Numerical value
LOCALSERVERPORT	Local port for connecting Network Agent to the iOS MDM service. The default port number is 9899. This setting is optional.	Numerical value
EXTERNALSERVERPORT	Port for connecting a device to the iOS MDM Server. The default port number is 443. This setting is optional.	Numerical value
EXTERNAL_SERVER_URL	External address of the client device on which iOS MDM Server is to be installed. This address will be used for connecting managed mobile devices to the iOS MDM service. The client device must be available for connection through iOS MDM. The address must not include the URL scheme and number of the port since these values will be added automatically. This setting is optional.	• Device FQDN (such as mdm.example.com) • Device NetBIOS name • Device IP address

Setting name	Setting description	Available values
WORKFOLDER	Workfolder of the iOS MDM Server. If no workfolder is specified, data will be written to the default folder. This setting is optional.	String value, for example, `WORKFOLDER=\"C:\work\"`
MTNCY	Use of iOS MDM Server by multiple virtual Servers. This setting is optional.	• 1 – The iOS MDM Server will be used by multiple virtual Administration Servers • Other value, or no value defined – The iOS MDM Server will not be used by multiple virtual Administration Servers.

Example:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

The iOS MDM Server installation settings are presented in detail in the Installing iOS MDM Server section (on page 138).

Use of iOS MDM Server by multiple virtual Servers

► *To enable the use of iOS MDM Server by multiple virtual Administration Servers:*

1. Open the system registry of the client device with iOS MDM Server installed (for example, locally, using the regedit command in the **Start** → **Run** menu).
2. Go to the following hive:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0
3. For the ConnectorFlags (DWORD) key, set the 02102482 value.
4. Go to the following hive:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0

5. For the ConnInstalled (DWORD) key, set the 00000001 value.
6. Restart the iOS MDM Server service.

Key values must be entered in the specified sequence.

Receiving an APNs certificate

When the Certificate Signing Request (CSR) is created at the first step of the APNs Certificate Wizard, its private key is stored in your device's RAM. Therefore, all wizard steps must be completed within a single session of the application.

► *To receive an APNs certificate:*

1. In the **Mobile devices** folder of the console tree, select an iOS MDM Server.

   The **Mobile devices** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the iOS MDM Server, select **Properties**.

   This opens the properties window of the iOS MDM Server.

3. In the properties window of the iOS MDM Server, select the **Certificates** section.

4. In the **Certificates** section, in the **Apple Push Notification certificate** group of settings, click the **Request new** button.

   The Receive APNs Certificate Wizard starts and the **Request new** window opens.

5. Create a Certificate Signing Request (hereinafter referred to as CSR request). To do this, perform the following actions:

   a. Click the **Create CSR** button.

   b. In the **Create CSR** window that opens, specify a name for your request, the names of your company and department, your city, region, and country.

   c. Click the **Save** button and specify a name for the file to which your CSR request will be saved.

   The private key of the certificate is saved in the device's memory.

6. Use your CompanyAccount to send the file with the CSR request you have created to Kaspersky Lab to be signed.

   > Signing of your CSR request will only be available after you upload to CompanyAccount portal a key that allows using Mobile Device Management feature.

   After your online request is processed, you will receive a CSR request file signed by Kaspersky Lab.

7. Send the signed CSR request file to Apple Inc. https://identity.apple.com/pushcert using a random Apple ID.

   > We recommend that you avoid using a personal Apple ID. Create a dedicated Apple ID to use it as corporate one. After you have created an Apple ID, link it with the organization's mailbox, not a mailbox of an employee.

   After your CSR request is processed in Apple Inc., you will receive the public key of the APNs certificate. Save the file to the disk.

8. Export the APNs certificate together with the private key created when generating the CSR request, in PFX file format. To do this, perform the following actions:

   a. In the **Request new APNs certificate** window, click the **Complete CSR** button.

   b. In the **Open** window, choose a file with the public key of the certificate, received from Apple Inc. as the result of CSR request processing, and press **Open** button.

   Certificate export process will be started.

   c. In the next window, enter private key password and click **OK**.

   This password will be used for the APNs certificate installation on the iOS MDM Server.

   d. In the **Save APNs Certificate** window, specify file name for APNs certificate, choose folder and click **Save**.

Private and public keys of the certificate are combined, and APNs certificate is saved in PFX format. After that, you can install the APNs certificate on the iOS MDM Server (see section "Installing an APNs certificate on an iOS MDM Server" on page 145).

For more detailed instructions on how to create a CSR and send it to Apple Inc., please refer to the Knowledge Base on the Kaspersky Lab Technical Support Service website (http://support.kaspersky.com/11077).

Installing an APNs certificate on an iOS MDM Server

After you have received the APNs certificate, you must install it on the iOS MDM Server.

► *To install the APNs certificate on the iOS MDM Server:*

1. In the **Mobile devices** folder of the console tree, select an iOS MDM Server.

   The **Mobile devices** folder is a subfolder of the **Advanced** folder by default.

2. In the context menu of the iOS MDM Server, select **Properties**.

   This opens the properties window of the iOS MDM Server.

3. In the properties window of the iOS MDM Server, select the **Certificates** section.

In the **Certificates** section, in the **Apple Push Notification certificate** group of settings click the **Install** button.

1. Select the PFX file that contains the APNs certificate.

2. Enter the password of the private key specified when exporting the APNs certificate (see section "Receiving an APNs certificate" on page 143).

As a result, the APNs certificate will be installed on the iOS MDM Server. The certificate details will be displayed in the properties window of the iOS MDM Server, in the **Certificates** section.

Issuing and installing a shared certificate on a mobile device

► *To issue a shared certificate to a user:*

1. In the console tree, in the **User accounts** folder, select a user account.

2. In the context menu of the user account, select **Install certificate**.

   The Certificate Installation Wizard starts. Follow the instructions of the Wizard.

When the Wizard finishes its operation, a certificate will be created and added to the list of the user's certificates.

The handed certificate will be downloaded by the user, along with the installation package that contains the iOS MDM profile.

After the mobile device is connected to the iOS MDM Server, the iOS MDM profile settings will be applied on the user's device. The administrator will be able to manage the device after connection.

The user's mobile device connected to the iOS MDM Server is displayed in the **Mobile Devices** subfolder within the **Mobile Device Management** folder of the console tree.

For instructions on how to hand certificates and manage iOS MDM mobile devices, please refer to the *Kaspersky Security Center Administrator's Guide*.

Adding an iOS MDM device to the list of managed devices

► *To add the iOS MDM device of a user to the list of managed devices using a link to App Store:*

1. In the console tree select the **User accounts** folder.

   By default, the **User accounts** folder is a subfolder of the **Advanced** folder.

2. Select the user account whose mobile device you want add to the list of managed devices.

3. In the context menu of the user account, select **Add device**.

The Add new device wizard starts running. In the **Certificate source** window of the Wizard, you have to specify the method of creation of the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate using any of the two methods:

- Create a shared certificate automatically, by means of Administration Server tools, then deliver the certificate to the device.
- Specify a shared certificate file.

4. In the **Device type** window of the Wizard, select **Link to App Store**.
5. In the **User notification method** window of the Wizard, configure notification of the mobile device user of certificate creation (with an SMS message or by email).
6. In the **Certificate info** window of the Wizard, click the **Finish** button to close the Certificate Installation Wizard.

After the Wizard finishes its activities, a link and a QR code will be sent to the user device thus allowing him or her to download Kaspersky Safe Browser from App Store. The user clicks the link or scans the QR code. After that, the operating system of the device prompts the user to accept Kaspersky Safe Browser installation. The user installs Kaspersky Safe Browser on the mobile device. When Kaspersky Safe Browser is installed, the user rescans the QR code to retrieve the Administration Server connection settings. When the QR code is rescanned in Safe Browser, the user retrieves the Administration Server connection settings and a shared certificate. The mobile device connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the latter is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

If Kaspersky Safe Browser has been previously installed on the mobile device, the user must independently enter the settings for connecting to the Administration Server. Using the scanning feature of Kaspersky Safe Browser, the user scans the QR code and retrieves the settings for device connection to the Administration Server. The user saves those settings on the device. After that, the mobile device automatically connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the latter is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree. In this case, Kaspersky Safe Browser will not be downloaded and installed again.

If an iOS MDM profile has previously been installed on an iOS MDM device, this device will be displayed twice on the list of devices in the **Mobile devices** folder (dubbed) after Kaspersky Safe Browser and the shared certificate are installed on the device. The device is dubbed on the list due to two shared (identification) certificates available on it.

Deploying a system for management via KES protocol using Self Service Portal

Kaspersky Security Center allows users to manage their mobile devices that are connected to Administration Server via KES protocol, by using Self Service Portal.

Self Service Portal supports mobile devices with the iOS and Android operating systems.

Deployment of a system for management via KES protocol by means of Self Service Portal includes the following steps:

1. Preparing for installation of Self Service Portal:
    a. The administrator installs Self Service Portal on the selected client device (see section "Installing Self Service Portal" on page 150).
    b. The administrator reports the address of Self Service Portal to the user.
2. Connecting the mobile device to Self Service Portal:
    a. The user opens the main page of the portal.

    Self Service Portal creates an installation package and then displays on the portal page a one-time link for downloading the installation package and a QR code in which the link is encoded. The installation package is required to install Network Agent on the device and apply corporate policies.

    b. The user goes to the installation package download page from the mobile device that should be added to Self Service Portal, downloads the installation package, and installs Network Agent on the mobile device.
    c. After Network Agent has been installed, the device connects to Administration Server.

As a result, the device will be added to the list of managed devices and the corporate policies will be applied to it. A link to information about connecting to the Administration Server is sent to the user's email address.

For information about how to add a device to Self Service Portal, please refer to the *Kaspersky Security Center Administrator's Guide*.

Adding a KES device to the list of managed devices

► *To add the KES device of a user to the list of managed devices using a link to Google Play™:*

1. In the console tree select the **User accounts** folder.

   By default, the **User accounts** folder is a subfolder of the **Advanced** folder.

2. Select the user account whose mobile device you want add to the list of managed devices.

3. In the context menu of the user account, select **Add device**.

   The Add new device wizard starts running. In the **Certificate source** window of the Wizard, you have to specify the method of creation of the shared certificate that Administration Server will use to identify the mobile device. You can specify a shared certificate using any of the two methods:

   - Create a shared certificate automatically, by means of Administration Server tools, then deliver the certificate to the device.
   - Specify a shared certificate file.

4. In the **Device type** window of the Wizard, select **Link to Google Play**.

5. In the **User notification method** window of the Wizard, define the settings for notification of the mobile device user of certificate creation (with an SMS message, by email, or by displaying the information when the Wizard is complete).

6. In the **Certificate info** window of the Wizard, click the **Finish** button to close the Certificate Installation Wizard.

After the Wizard finishes its activities, a link and a QR code will be sent to the mobile device of the user thus allowing him or her to download Kaspersky Endpoint Security from Google Play. The user proceeds to Google Play by using the link or by scanning the QR code. After that, the operating system of the device prompts the user to accept Kaspersky Endpoint Security for Android installation. After Kaspersky Endpoint Security for Android is downloaded and installed, the mobile device connects to the Administration Server and downloads a shared certificate. After the certificate is installed on the mobile device, the latter is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree.

If Kaspersky Endpoint Security for Android has already been installed on the device, the user has to receive the Administration Server connection settings from the administrator and then enter them on his or her own. After the connection settings are defined, the mobile device connects to the Administration Server. The administrator issues a shared certificate for the device and sends the user an email message or an SMS message with a user name and a password for the certificate download. The user downloads and installs the shared certificate. After the certificate is installed on the mobile device, the latter is displayed in the **Mobile devices** folder, which is a subfolder of the **Mobile Device Management** folder of the console tree. In this case, Kaspersky Endpoint Security for Android will not be downloaded and installed again.

Installing Self Service Portal

This section describes preparation to Self Service Portal installation, as well as the installation steps.

The device on which Self Service Portal deployment is planned, must meet the following requirements:

- Administration Server must be installed on the device (see section "Deploying Administration Server" on page 49).
- iOS MDM Server must be installed on the device (see section "Deploying a system for management via iOS MDM" on page 136).

Self Service Portal installation requires local administrator rights on the device on which installation is to be performed.

► *To install Self Service Portal on a local device:*

1. In the console tree, select the Self Service Portal folder, which is nested in the **Mobile Device Management** folder.
2. In the workspace of the folder, click the **Install Self Service Portal** button.
3. In the **Current application versions** window, select and download the relevant distribution package by clicking the **Download distribution package** button.
4. Run the file that you downloaded.

   The Distribution Package Extraction Wizard starts. Follow the Wizard's steps.
5. Unpack the distribution package to the relevant folder.
6. In the folder that you specified, run the install.exe file.

   The Application Setup Wizard starts. Follow the instructions of the Wizard.

You can also run the install.exe file from the CD containing the Kaspersky Security Center 10 Web Console distribution package.

> Installation of Self Service Portal from the distribution package downloaded from the Internet is no different than installation from the installation CD.

Step 1.
Reviewing the License Agreement

At this step of the Setup Wizard, you should read the License Agreement, which is to be concluded between you and Kaspersky Lab.

Please, read the End User License Agreement carefully. If you accept all of the provisions, select the **I accept the terms of the License Agreement** check box. Installation continues.

If you do not accept the End User License Agreement, cancel the application installation by clicking the **Cancel** button.

> Remote installation of Self Service Portal using an installation package or local installation in non-interactive mode means automatic acceptance of the terms of the License Agreement related to the application that you are installing. You can view the License Agreement in the application distribution kit (the file license.txt) or on Technical Support website of Kaspersky Lab.

Step 2. Connecting to Kaspersky Security Center

Select the mode for connecting Self Service Portal to Kaspersky Security Center. The following connection options are available:

- **Use Apache server installed on local device**. If this option is selected, Self Service Portal is connected to Kaspersky Security Center via the Apache server installed on a local device (you can select Apache server installation at the next step of the Wizard).

- **Use Apache server installed on remote device**. You can select this option if an Apache server is already installed on a remote device. In this case, only the server part of Self Service Portal will be installed locally. To connect Self Service Portal to Kaspersky Security Center, the client part of Self Service Portal must be installed on the remote device. If you select this option, the Setup Wizard proceeds to Step 7 (see section "Step 6. Selecting ports" on page 155).

► *To install the client part of Self Service Portal on a remote device running Linux,*

run the following files on the remote device, depending on the operating system type:

- For 32-bit systems:
  - kscwebconsole-10.<build_number>.i386.rpm;
  - kscwebconsole_10.<build_number>_i386.deb.
- For 64-bit systems:
  - kscwebconsole-10.<build_number>.x86_64.rpm;
  - kscwebconsole_10.<build_number>_x86_64.deb.

Run the file with the rpm extension if an RPM-based operating system is installed on the device. Run the file with the deb extension if a DEB-based operating system is installed on the device.

Step 3. Selecting the destination folder

Specify the target folder for installation of Self Service Portal. By default, this will be <Drive>:\Program Files\Kaspersky Lab\Kaspersky Security Center Self Service Portal. If this folder does not exist, it will be created automatically. You can change the destination folder by using the **Browse** button.

Step 4. Selecting the Apache server installation mode

If no Apache server is installed on the device, at this step, the Setup Wizard prompts you to install Apache HTTP Server 2.4.25.

By default, Apache HTTP Server 2.4.25 is selected as the installation option. If you do not want to install the Apache server through the Kaspersky Security Center 10 Web Console Setup Wizard, clear the **Install Apache HTTP Server 2.4.25** check box.

> Apache Server installation may prompt you to restart the device.

Step 5. Installing Apache Server

At this step of the Setup Wizard, installation and configuration of Apache HTTPS Server 2.4.25 are performed.

Before installing, specify the certificate that Self Service Portal will use to connect to the Apache server. Select one of the following options:

- **Generate new certificate**. Create a new certificate to work via HTTPS. In this case, a self-signed certificate will be created to work via HTTPS.
- **Choose existing**. Use an existing certificate for working via HTTPS. Specify a certificate using one of the following methods:
  - **Select certificate file**. Select an existing certificate file by clicking the **Browse** button.
  - **Select a private key**. Specify a certificate using the file of its private key, by clicking the **Browse** button.

> Using self-signed or user-selected untrusted certificates may cause problems with access to Self Service Portal on some devices. Such issues can be solved by adding the root certificate to the list of trusted ones on the device.

If necessary, you can configure Self Service Portal to work via HTTP instead of HTTPS. For more details on how to configure Self Service Portal to work via HTTP, please refer to the Knowledge Base of Kaspersky Lab Technical Support at http://support.kaspersky.com/11452.

After you have selected a certificate, click the **Next** button. As a result, installation of Apache HTTPS Server 2.4.25 starts. Follow the instructions of the Wizard.

Step 6. Selecting the ports

Define the following settings:

- Number of the SSL port for encrypted connection of the device to the Administration Server. The default port number is 13291.
- Number of the port for the device connection to the Apache server. The default port number is 9000.
- Address of the device with Administration Server installed. The default address is localhost.

  If the device on which Kaspersky Security Center 10 Web Console and Self Service Portal are to be installed is in DMZ, select the **Connection gateway** check box and specify the connection gateway address in the **Server address** field.
- Number of the port for the device connection to Kaspersky Security Center 10 Web Console. The default port number is 8080.
- Number of the port for the device connection to Self Service Portal. The default port number is 8081.

When Kaspersky Security Center 10 Web Console and Self Service Portal are installed, you can change the default port numbers (see section "Changing the port number for device connection" on page 88).

Step 7. Selecting an account

Specify the user's domain account under which installation packages will be downloaded to users' mobile devices by means of QR codes. The account must be specified in *<Domain name>\<Account name>* format.

Click the **Test** button to test the Administration Server connection.

Step 8. Running installation of Self Service Portal

Click the **Start** button to run the installation of Self Service Portal.

The installation process is displayed on the Wizard page.

Step 9. Finishing installation of Self Service Portal

If Apache 2 Server, version 2.4.25 or later, has been installed on the device before Self Service Portal installation, or if automatic installation of the Apache server returned an error, at this step of the Setup Wizard you are prompted to open the file that provides instructions for the Apache Server configuration. To open the text file with instructions after the Wizard completes its operation, select the **Open readme.txt** check box.

To complete the Setup Wizard, click the **Finish** button.

Configuring SMS delivery in Kaspersky Security Center

Kaspersky Security Center can be used for sending SMS notifications to mobile devices users.

SMS delivery may be used in the following cases:

- If the administrator needs to receive SMS notifications of events occurring in the operation of Administration Server and applications installed on client devices.
- To install applications to users' mobile devices. A mobile device user receives an SMS message that contains a link to download an application required to install.
- To notify employees.

Deployment of SMS delivery is performed as follows:

1. The administrator installs Kaspersky SMS Broadcasting utility to an Android mobile device.

   > Kaspersky SMS Broadcasting utility can be installed to mobile devices under Android only.

2. After Kaspersky SMS Broadcasting utility is installed to the mobile device, the administrator synchronizes the mobile device with Administration Server.
3. The administrator assigns the mobile device on which the Kaspersky SMS Broadcasting utility is installed, as the SMS sender in Administration Console.

In this section:

Retrieving and installing Kaspersky SMS Broadcasting utility 158

Synchronization of a mobile device with Administration Server 159

Assigning a mobile device as the SMS sender 160

Retrieving and installing Kaspersky SMS Broadcasting utility

Kaspersky SMS Broadcasting utility makes part of the installation package of Kaspersky Endpoint Security 10 for Mobile Devices. You can download the installation package of Kaspersky Endpoint Security 10 for Mobile Devices from the Kaspersky Lab website.

► *To install Kaspersky SMS Broadcasting utility:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.

   The **Remote installation** folder is a subfolder of the **Advanced** folder by default.

2. Click the **Additional actions** button and select **Manage packages of mobile applications** from the drop-down list.

3. In the **Mobile applications packages management** window select the package of a mobile application containing Kaspersky SMS Broadcasting utility.

   If no package has been yet created, click the **New** button and create a mobile application package for Kaspersky SMS Broadcasting utility.

4. In the **Mobile applications packages management** window click the **Publish on web server** button.

   A link for downloading the mobile applications package with Kaspersky SMS Broadcasting utility will be published on a web server.

5. In the **Mobile applications packages management** window click the **Send by email** button to send a mobile device user the link for downloading the mobile applications package containing the Kaspersky SMS Broadcasting utility.

6. Download the mobile applications package containing the Kaspersky SMS Broadcasting utility from the web server to the mobile device.

7. Install Kaspersky SMS Broadcasting utility using the standard tools of your mobile device.

You can also download the Kaspersky SMS Broadcasting utility to your mobile device from the Kaspersky Lab website, or connect your mobile device to a client device and copy the Kaspersky SMS Broadcasting utility that has already been downloaded.

Synchronization of a mobile device with Administration Server

► *To synchronize a mobile device with Administration Server:*

1. In the console tree of Kaspersky Security Center, from the context menu of the **Administration Server** folder select **Properties**.

   The properties window of Administration Server opens.

2. In the properties window of Administration Server, in the **Settings** section select the **Open port for mobile devices** check box.

3. In the **Settings** section, in the **Port for mobile devices** field specify a port for synchronization of the mobile device with Administration Server. The default port number is 13292.

4. Run Kaspersky SMS Broadcasting utility on the mobile device.

5. In the main window of Kaspersky SMS Broadcasting utility press the **Synchronization settings** button.

6. In the **Synchronization settings** window, in the **Server address** field specify the IP address of Administration Server.

7. In the **Port** field specify a port for connect to Administration Server. The default port number is 13292.

8. Click **OK**.

When the mobile device is synchronized with Administration Server, you can assign this mobile device the SMS message sender.

Assigning a mobile device as the SMS sender

► *To assign a mobile device as the SMS sender:*

1. In the console tree, select the node with the name of the required Administration Server.
2. In the workspace of the node, select the **Events** tab.
3. Click the **Configure notifications and event export** link and select **Set up list of SMS senders** in the drop-down list.

   This opens the event properties window, displaying the **SMS senders** section.
4. Click the **Add** button in the **SMS senders** section.

   The **Select device** window opens.
5. In the **Select device** window specify a mobile device that will be used as the SMS sender.
6. Click **OK**.

Kaspersky SMS Broadcasting utility must be installed on the device assigned as the SMS sender.

Network load

This section contains information about the volume of network traffic that client devices and the Administration Server exchange when some of the key administrative scenarios are in progress.

Main load on the network is caused by the following administrative scenarios in progress:

- Initial deployment of anti-virus protection.
- Initial update of anti-virus databases.
- Client device synchronization with the Administration Server.
- Regular update of anti-virus databases.
- Event processing on client devices by the Administration Server.

In this section:

Initial deployment of anti-virus protection 162

Initial update of anti-virus databases 163

Synchronizing a client with the Administration Server 163

Additional update of anti-virus databases 165

Processing of events from clients by Administration Server 166

Traffic per 24 hours 167

Initial deployment of anti-virus protection

This section provides information about traffic rates after Network Agent 10 and Kaspersky Endpoint Security 10 for Windows are installed on the client device (see table below).

Network Agent is installed through forced installation, when the files required for installation are copied by the Administration Server to a shared folder on the client device. After installation, the Network Agent retrieves the distribution package of Kaspersky Endpoint Security 10 for Windows using connection to the Administration Server.

Table 10. Traffic

Scenario	Installing Network Agent on a single client device	Installing Kaspersky Endpoint Security 10 for Windows on a single client device (with databases updated)	Concurrent installation of the Network Agent and Kaspersky Endpoint Security 10 for Windows
Traffic from the client device to the Administration Server, KB	386.70	1,841.3	2,253.8
Traffic from the Administration Server to the client computer, KB	14,801.13	269,994.5	284,768.7
Total traffic (for a single client device), KB	15,187.83	271,835.8	287,022.5

After the Network Agents are installed on the client devices, you can assign one of the devices in the administration group to act as update agent. It is used for distribution

of installation packages. In this case, traffic volume transferred during initial deployment of anti-virus protection varies considerably depending on whether you are using IP multicasting.

If you are using IP multicasting, installation packages are sent to all running devices in the administration group only once. Thus, total traffic becomes N times smaller, where N stands for the total number of running devices in the administration group. If you are not using IP multicasting, the total traffic is identical to the traffic calculated as if the distribution packages are downloaded from the Administration Server. However, the package source is the update agent, not the Administration Server.

Initial update of anti-virus databases

This section provides traffic rates calculated for the first run of the database update task on a client device (see table below). The data in the table may vary slightly depending upon the current anti-virus database version.

Table 11. Traffic

Scenario	Initial update of anti-virus databases
Traffic from the client device to the Administration Server, KB	1,357.1
Traffic from the Administration Server to the client computer, KB	33,917.0
Total traffic (for a single client device), KB	35,274.1

Synchronizing a client with the Administration Server

This scenario describes the state of the administration system when intensive data synchronization occurs between a client device and the Administration Server. Client devices connect to the Administration Server with the interval defined by the administrator. The Administration Server compares the status of data on the client device with that on the Administration Server, logs the details of the last client device connection to the database, and synchronizes data.

This section contains information about traffic values for basic administration scenarios when connecting a client to the Administration Server (see table below). The data in the table may vary slightly depending upon the current anti-virus database version.

Table 12. Traffic

Scenario	Traffic from client devices to the Administration Server, KB	Traffic from the Administration Server to client devices, KB	Total traffic (for a single client device), KB
Initial synchronization before databases were updated on the client device	368.6	463.7	832.3
Initial synchronization after databases were updated on the client device	1,748.3	34,388.3	36,136.6
Synchronization when no changes were made to the client device and the Administration Server	8.7	6.6	15.3
Synchronization after changing the value of a setting in a group policy	11.1	13.3	24.4
Synchronization after changing the value of a setting in a group task	10.0	12.5	22.5
Forced synchronization when no changes were made to the client device	47.3	15.5	62.8

Overall traffic volume varies considerably depending on whether or not multicast IP delivery is used within administration groups. If you are using IP multicasting, the total traffic rate for this group decreases approximately by N times, where N stands for the total number of running devices in the administration group.

The volume of traffic at initial synchronization before and after an update of the databases is specified for the following cases:

- Installing Network Agent and a security application on the client device
- Moving the client device to an administration group
- Applying to the client device a policy and tasks that have been created for the default group

The table specifies traffic rates in case of modifying a protected setting comprised in the Kaspersky Endpoint Security policy settings. Data for other policy settings may differ from those displayed in the table.

Additional update of anti-virus databases

This section contains information about traffic rates in case of an incremental update of anti-virus databases 20 hours after the previous update (see table below). The data in the table may vary slightly depending upon the current anti-virus database version.

Table 13. Traffic

Scenario	Incremental update of anti-virus databases
Traffic from the client device to the Administration Server, KB	436.9
Traffic from the Administration Server to the client computer, KB	9,979.2
Total traffic (for a single client device), KB	10,416.1

Traffic volume varies considerably depending on whether or not multicast IP delivery is used within administration groups. If you are using IP multicasting, the total traffic rate for this group decreases approximately by N times, where N stands for the total number of running devices in the administration group.

Processing of events from clients by Administration Server

This section provides traffic rates in case a client device encounters a "Virus detected" event, which is then sent to the Administration Server and logged to the database (see table below).

Table 14. Traffic

Scenario	Data transfer to Administration Server upon a "Virus detected" event	Data transfer to Administration Server upon nine "Virus detected" events
Traffic from the client device to the Administration Server, KB	27.2	100.4
Traffic from the Administration Server to the client computer, KB	25.8	52.5
Total traffic (for a single client device), KB	53.0	152.9

Data in the table may vary slightly depending upon the current version of the anti-virus application and the events that are defined in its policy for registration in the Administration Server database.

Traffic per 24 hours

This section provides per-day traffic rates during the administration system operation under a "quiet" condition, i.e., when no changes are made to data both by client devices and by the Administration Server (see table below).

Data stated in the table describe the network's condition after the standard installation of Kaspersky Security Center and the closing of the Quick Start Wizard. The interval of the client device synchronization with the Administration Server was 20 minutes; updates were downloaded to the Administration Server repository every hour.

Table 15. Traffic

Scenario	"Idle" state of the administration system
Traffic from the client device to the Administration Server, KB	2,162.2
Traffic from the Administration Server to the client computer, KB	51,000.2
Total traffic (for a single client device), KB	53,162.4

Rate of adding Kaspersky Endpoint Security events to the database

This section contains examples showing various speed rates for filling up the Administration Server database with events that occur in the operation of managed applications.

Information about events in the operation of managed applications is transferred from a client device and logged to the Administration Server database.

(Ne*Nh) events per day are added to the database (see table below). Here Nh is the number of client devices where managed applications are installed, Ne is the number of events per day that are informed of by a managed application installed on a client device.

Table 16. Rate of database filling with events

Number of devices where managed applications are installed	Number of events added to the database per day
100	≤ 2,000
1,000	≤ 20,000
10,000	≤ 200,000

The table contains data for standard run mode of managed applications allowing not more than 20 events per day to be received from each client device.

The maximum number of events stored in the database is defined in the **Events storage** section of the Administration Server properties window. By default, the database contains not more than 400,000 events.

Contacting the Technical Support Service

This section provides information about the ways and conditions for providing you technical support.

In this section:

How to obtain technical support 169

Technical support by phone 170

Technical Support via Kaspersky CompanyAccount 170

How to obtain technical support

If you do not find a solution to your problem in the documentation or in other sources of information about the application (see section "Sources of information about the application" on page 13), we recommend that you contact the Kaspersky Lab Technical Support Service. Technical Support Service experts will answer your questions about installing and using the application.

Technical support is only available to users who purchased the commercial license. Users who have received a trial license are not entitled to technical support.

Before contacting the Technical Support Service, we recommend that you read through the technical support rules (http://support.kaspersky.com/support/rules).

You can contact the Technical Support Service in one of the following ways:

- By calling the Technical Support Service by phone (http://support.kaspersky.com/support/contacts).
- By sending a request to the Kaspersky Lab Technical Support Service using the Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

Technical support by phone

In most regions of the world, you can call experts at the Kaspersky Lab Technical Support Service. You can receive information about how to obtain technical support in your region and the contact information of the Technical Support Service on the website of the Kaspersky Lab Technical Support Service (http://support.kaspersky.com/b2c).

Before contacting the Technical Support Service, please read the technical support rules (http://support.kaspersky.com/support/rules).

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab experts through online requests. The Kaspersky CompanyAccount portal allows you to monitor the progress of electronic request processing by Kaspersky Lab experts and store the history of electronic requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English.
- Spanish.
- Italian.
- German.
- Polish.
- Portuguese.
- Russian.
- French.
- Japanese.

To learn more about Kaspersky CompanyAccount, please visit the Technical Support Service website (http://support.kaspersky.com/faq/companyaccount_help).

Glossary

A

Active key

Key that is used at the moment to work with the application.

Additional key

A key that certifies the right to use the application but is not currently being used.

Administration Console

A Kaspersky Security Center component that provides a user interface for the administrative services of Administration Server and Network Agent.

Administration group

A set of devices grouped by function and by installed Kaspersky Lab applications. Devices are grouped as a single entity for the convenience of management. A group can include groups. A group can contain group policies and group tasks for each installed application.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. Administration Server can also be used to manage these applications.

Administration Server certificate

Certificate used for Administration Server authentication during Administration Console connection and data exchange with client devices. The Administration Server certificate is created and

installed on Administration Server in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder.

Administration Server client (Client device)

A device, server, or workstation on which Network Agent is installed and managed Kaspersky Lab applications are running.

Administrator's workstation

Device with an installed component that provides an application management interface.
For anti-virus products, this component is Anti-Virus Console, and for Kaspersky Security Center it is Administration Console.

The administrator's workstation is used to configure and manage the server portion of the application. For Kaspersky Security Center it is used to build and manage a centralized anti-virus protection system for a corporate LAN based on Kaspersky Lab applications.

Anti-virus databases

Databases that contain information about computer security threats that are known to Kaspersky Lab at the time of release of the anti-virus databases. Records that are contained in anti-virus databases allow detecting malicious code in scanned objects. The anti-virus databases are created by Kaspersky Lab experts and updated every hour.

Application management plug-in

A specialized component that provides the interface for application management through Administration Console. Each application has its own management plug-in. It is included in all Kaspersky Lab applications that can be managed by using Kaspersky Security Center.

Application settings

Application settings which are general for all types of its tasks and regulating its operation in general, for example, application performance, logging, and Backup settings.

Available update

A package of updates for the modules of a Kaspersky Lab application including a set of urgent patches released during a certain time interval, and modifications to the application architecture.

B

Backup folder

Special folder for storage of Administration Server data copies created using the backup utility.

Backup of Administration Server data

Copying of the Administration Server data for backup and subsequent restoration performed by using the backup utility. The utility can save:

- Information database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server).
- Configuration details of the administration group structure and client devices.
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates).
- Administration Server certificate.

C

Centralized application management

Remote application management using the administration services provided in Kaspersky Security Center.

Configuration profile

Policy that contains a collection of settings and restrictions for an iOS MDM mobile device.

D

Direct application management

Application management through a local interface.

E

EAS device

A mobile device connected to Administration Server through the Exchange ActiveSync protocol.

Event importance level

Property of an event encountered during the operation of a Kaspersky Lab application.
There are four importance levels:

- Critical event.
- Functional failure.
- Warning.
- Info.

Events of the same type can have different importance levels depending on the situation in which the event occurred.

F

Forced installation

Method for remote installation of Kaspersky Lab applications that allows you to install software on specific client devices. For a successful forced installation, the account used for this task must have sufficient rights to run applications remotely on client devices. This method is recommended for software installation on devices running Microsoft Windows NT/2000/2003/XP and supporting that feature, or on devices running Microsoft Windows 98/Me with Network Agent installed.

G

Group task

A task defined for an administration group and performed on all client devices included in that administration group.

I

Incompatible application

Anti-virus application of another vendor or a Kaspersky Lab application that does not support management through Kaspersky Security Center.

Installation package

A set of files created for remote installation of a Kaspersky Lab application by using the Kaspersky Security Center remote administration system. The installation package contains a range of settings needed to install the application and get it running immediately after installation.

Settings correspond to application defaults. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit.

iOS MDM device

Mobile device running iOS and managed by an iOS MDM Server (see section "iOS MDM Server" on page 185).

iOS MDM profile

Collection of settings for connecting iOS mobile devices to Administration Server. The user installs an iOS MDM profile to a mobile device, after which this mobile device connects to Administration Server.

iOS MDM Server

A component of Kaspersky Security Center that is installed on a client device, allowing connection of iOS mobile devices to the Administration Server and management of iOS mobile devices through Apple Push Notifications (APNs).

K

Kaspersky Lab update servers

HTTP and FTP servers of Kaspersky Lab from which Kaspersky Lab applications download database and application module updates.

Kaspersky Security Center administrator

The person managing the application operations through the Kaspersky Security Center system of remote centralized administration.

Kaspersky Security Center operator

A user who monitors the status and operation of a protection system managed with Kaspersky Security Center.

Kaspersky Security Center System Health Validator (SHV)

A component of Kaspersky Security Center application designed for checking the operating system's operability in case of concurrent operation of Kaspersky Security Center and Microsoft NAP.

Kaspersky Security Center Web Server

A component of Kaspersky Security Center installed together with Administration Server. Web Server is designed for transfer of stand-alone installation packages, iOS MDM profiles, and files from a shared folder over the network.

Key file

A file in xxxxxxxx.key format that makes it possible to use a Kaspersky Lab application under a trial or commercial license. The application can be used only with a key file.

L

License term

Time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

Local task

A task defined and running on a single client device.

Logon script-based installation

Method for remote installation of Kaspersky Lab applications that allows you to link the start of a remote setup task to specified user account or accounts. When the user signs up to the domain, the system attempts to install the application on the corresponding client device. This method is recommended for installation of company-specific applications on devices running Microsoft Windows 98/Me.

M

Microsoft Exchange Mobile Devices Server

A component of Kaspersky Security Center that allows you to connect Exchange ActiveSync mobile devices to the Administration Server. Installed on a client device.

Mobile device server

A component of Kaspersky Security Center that provides access to mobile devices and allows managing them through Administration Console.

N

Network Agent

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky Lab applications that are installed on a specific network node (workstation or server). This component is common for all of the company's products for Windows.
Special versions of Network Agent have been developed for Kaspersky Lab products for Novell, Unix, and Mac.

P

Policy

A policy determines the settings of an application and manages the access to configuration of an application installed on computers within an administration group. An individual policy must be created for each application. You can create an unlimited number of various policies for applications installed on computers in each administration group, but only one policy can be applied to each application at a time within an administration group.

Profile

Collection of settings of Exchange ActiveSync mobile devices that define their behavior when connected to a Microsoft Exchange Server.

Protection status

Current protection status, which reflects the level of device security.

Provisioning profile

Collection of settings for applications' operation on iOS mobile devices. A provisioning profile contains information about the license; it is linked to a specific application.

R

Remote installation

Installation of Kaspersky Lab applications through tools provided by Kaspersky Security Center.

Restoration of Administration Server data

Restoration of Administration Server data from the information saved in Backup by using the backup utility. The utility can restore:

- Information database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server).
- Configuration details of the administration group structure and client devices.
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates).
- Administration Server certificate.

T

Task

Functions performed by Kaspersky Lab application are implemented as tasks, such as Real-time file protection, Full device scan, and Database update.

Task for specific devices

A task assigned to a set of client devices from arbitrary administration groups and performed on those devices.

Task settings

Task-specific application settings.

U

Update

The procedure of replacing or adding new files (databases or application modules) that are retrieved from Kaspersky Lab update servers.

Update agent

Device with Network Agent installed, which is used for update distribution, remote installation of applications, collection of information about devices in an administration group and/or broadcasting domain. Update agents are designed to reduce the load on the Administration Server during update distribution and to optimize network traffic. Update agents can be assigned automatically, by the Administration Server, or manually, by the administrator.

V

Virus activity threshold

Maximum allowed number of events of the specified type within a limited time; when this number is exceeded, it is interpreted as increased virus activity and as a threat of a virus attack.
This feature is important during periods of virus outbreaks because it enables administrators to respond in a timely manner to virus attack threats.

AO Kaspersky Lab

Kaspersky Lab is an internationally renowned vendor of systems for computer protection against various types of threats, including viruses, malware, spam, network and hacker attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). In Russia, according to IDC, Kaspersky Lab is the first choice among all vendors of computer protection systems for home users (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3,000 qualified experts.

Products. Kaspersky Lab products provide protection for all systems, ranging from home computers to large corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers solutions and technologies for protection and control of workstations and mobile devices, virtual machines, file servers and web servers, mail gateways, and firewalls. The company's portfolio also includes dedicated products aimed at protection against DDoS attacks, protection of environments managed with industrial control systems, and fraud prevention. Used in conjunction with the centralized management tools of Kaspersky Lab, these solutions ensure effective automated protection against computer threats for organizations of any scale. Kaspersky Lab products are certified by major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and add the corresponding signatures to databases used by Kaspersky Lab applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that the program kernel of Kaspersky Anti-Virus is integrated in products made by many other software vendors, including:

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, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2014, tests and research conducted by the renowned Austrian anti-virus lab AV-Comparatives rated Kaspersky Lab as one of the two leaders in the number of Advanced+ certificates awarded, which earned the company the Top Rated certificate. However, the main achievement of Kaspersky Lab is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website	http://www.kaspersky.com	
Virus encyclopedia:	https://securelist.com	
Anti-Virus Lab:	https://newvirus.kaspersky.com/ unknown files and websites)	(for scanning
Kaspersky Lab web forum:	http://forum.kaspersky.com	

Enhanced protection with Kaspersky Security Network

Kaspersky Lab offers an extra layer of protection to users through the Kaspersky Security Network. This protection method is designed to combat advanced persistent threats and zero-day attacks. Integrated cloud technologies and the expertise of Kaspersky Lab virus analysts make Kaspersky Endpoint Security the unsurpassed choice for protection against the most sophisticated network threats.

Details on enhanced protection in Kaspersky Endpoint Security are available on the Kaspersky Lab website.

Information about third-party code

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.

Trademark notices

The registered trademarks and service marks are the property of their owners.

Active Directory, ActiveSync, Edge, Internet Explorer, Hyper-V, Microsoft, MultiPoint, SharePoint, SQL Server, Windows, Windows Server, Windows Phone, and Windows Vista are trademarks of Microsoft Corporation registered in the United States and elsewhere.

Android, Chrome, and Google Play are trademarks owned by Google, Inc.

Apache and the Apache feather logo are trademarks owned by the Apache Software Foundation.

Apple, App Store, Leopard, Mac, Mac OS, macOS, Safari, Snow Leopard, OS X, and Tiger are trademarks of Apple Inc. registered in the United States and elsewhere.

Cisco is a registered trademark or trademark of Cisco Systems, Inc. and / or its affiliates in the United States and certain other countries.

Citrix and XenServer are trademarks of Citrix Systems, Inc. and / or its subsidiaries registered in the United States Patent Office and elsewhere.

Debian is a registered trademark of Software in the Public Interest, Inc.

Intel, Core and Xeon are trademarks of Intel Corporation in the U.S. and / or other countries.

CentOS, Fedora and Red Hat Enterprise Linux are trademarks of Red Hat Inc. registered in the United States and elsewhere.

Firefox is a registered trademark of the Mozilla Foundation.

FreeBSD is a registered trademark of FreeBSD foundation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Linux is a trademark owned by Linus Torvalds and registered in the U.S. and elsewhere.

Novell and Netware are trademarks of Novell Inc. registered in the United States and elsewhere.

SUSE is a trademark of SUSE LLC registered in the United States and elsewhere.

Ubuntu is a registered trademark of Canonical Ltd.

UNIX is a trademark registered in the U.S. and elsewhere and is used under license from X/Open Company Limited.

VMware is a trademark of VMware, Inc., or a trademark owned by VMware, Inc. and registered in the U.S. and elsewhere.

Symbian is a trademark owned by the Symbian Foundation Ltd.

The BlackBerry trademark is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

Index

A

Active Directory 103

Addition

Administration Server 88, 96

Administration Console 59

Administration groups 96

Administration Server 59, 67

B

Building defense 41

C

Cisco Network Admission Control 59

Configuration

kpd-file 114

Custom installation 57

D

Database 62

Deployment schemes 41

Distribution of installation package 113, 114

E

exec 103

F

File with application description 114

Forced installation 100

I

Installation

- Active Directory 97, 103
- custom 57
- forced 100
- Kaspersky Security Center 52
- local 123
- logon script 100
- remote 97
- selection of components 59
- silent mode 130
- slave Administration Server 105
- stand-alone package 97, 131
- task 97

Installation package 95, 111

- distribution 113, 114

K

klbackup 50

klsrvswch 61

kpd-file 114

L

Local System Account 61

Logon script 100

M

Mobile device support 59

Mobile devices 66

N

Network Agent 59, 67

installation 93, 125

Network poll 92

Network Size 60

P

Packages 111

Policy Server 59, 67

Ports 53

R

Remote installation preparation utility 97, 106, 118

Remote Installation Wizard.....106

Removal

task.....109

Removing

Kaspersky Security Center.....77

Reports 107

riprep 118

S

Service

Administration Server 67

Network Agent.....67

Policy Server.....67

Shared folder.....65

Slave Servers

addition.....96

SNMP agent.....59

SQL-server.....62

Stand-alone installation package 97, 131

Standard installation 56

Stress testing.....41

T

Task....100

U

Update agents....92, 93, 95, 114

Updating the application....50

User account....61