Dear User,

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

Attention! 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 thereof 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. The latest version of this document can be found on the Kaspersky Lab website, at http://www.kaspersky.com/docs.

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: 11/19/2013

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

http://www.kaspersky.com
http://support.kaspersky.com
TABLE OF CONTENTS

ABOUT THIS GUIDE ................................................................................. 6
  In this document ................................................................................. 6
  Document conventions ...................................................................... 8

SOURCES OF INFORMATION ABOUT THE APPLICATION ................. 9
  Sources of information for independent research .............................. 9
  Discussing Kaspersky Lab applications on the forum ....................... 10
  Contacting the Technical Writing and Localization Unit ................. 10

KASPERSKY SECURITY CENTER .......................................................... 11

APPLICATION ARCHITECTURE .......................................................... 12

HARDWARE AND SOFTWARE REQUIREMENTS .................................. 13

INFORMATION ABOUT ADMINISTRATION SERVER PERFORMANCE .... 16

SELECTING A STRUCTURE OF AN ORGANIZATION PROTECTION SYSTEM 17

TYPICAL SCHEMES OF PROTECTION SYSTEM DEPLOYMENT ............. 18

DEPLOYING A PROTECTION SYSTEM WITHIN AN ORGANIZATION ...... 19
  Deploying a protection system using Administration Console within an organization ................................................. 19
  Deploying a protection system using Kaspersky Security Center Web-Console within an organization ................. 19
  Deploying a protection system manually within an organization ... 20

DEPLOYING A PROTECTION SYSTEM ON A CLIENT ORGANIZATION'S NETWORK .......................................................... 21
  Deploying a protection system using Administration Console on a client organization's network ......................... 21
  Deploying a protection system using Kaspersky Security Center Web-Console in a client organization's network .......................................................... 22
  Deploying a protection system on a client organization's network manually .......................................................... 22

DEPLOYING ADMINISTRATION SERVER ............................................ 24
  Stages of deploying Administration Server within an enterprise ......................... 24
  Steps of Administration Server deployment for protection of a client organization's network ......................... 24
  Upgrading the previous version of Kaspersky Security Center .............. 25
  Installing and removing Kaspersky Security Center .......................... 25
    Preparing for installation .................................................................. 26
    Standard installation ........................................................................ 27
    Custom installation ......................................................................... 28
    Installation in non-interactive mode .................................................. 33
    Changes in the system after installing the application ...................... 35
    Removing the application ................................................................ 37
  Installing Administration Console on the administrator's workstation .......................................................... 37
  Installing and configuring Kaspersky Security Center SHV ............... 37
  Installing Kaspersky Security Center Web-Console .......................... 38
    Step 1. Reviewing the License Agreement ........................................ 38
    Step 2. Selecting the destination folder ............................................. 39
    Step 3. Selecting the ports ............................................................... 39
    Step 4. Connecting to Kaspersky Security Center ............................ 39
    Step 5. Selecting the Apache Server installation mode .................... 39
    Step 6. Installing Apache Server ..................................................... 40
    Step 7. Starting installation of Kaspersky Security Center Web-Console .......................................................... 40
    Step 8. Completing installation of Kaspersky Security Center Web-Console .......................................................... 40
  Configuring interaction between Administration Server and Kaspersky Security Center Web-Console .................. 40

CONFIGURING A PROTECTION SYSTEM FOR A CLIENT ORGANIZATION'S NETWORK .......................................................... 42
  Defining an Update Agent. Configuring Update Agent ....................... 42
  Local installation of the Network Agent to Update Agent .................. 43
  Requirements to installation of applications on computers of a client enterprise .......................................................... 44
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE OF ADDING KASPERSKY ENDPOINT SECURITY EVENTS TO THE DATABASE</td>
<td>76</td>
</tr>
<tr>
<td>CONTACTING TECHNICAL SUPPORT SERVICE</td>
<td>77</td>
</tr>
<tr>
<td>- How to obtain technical support</td>
<td>77</td>
</tr>
<tr>
<td>- Technical support by phone</td>
<td>77</td>
</tr>
<tr>
<td>- Obtaining technical support via Kaspersky CompanyAccount</td>
<td>77</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>79</td>
</tr>
<tr>
<td>KASPERSKY LAB ZAO</td>
<td>84</td>
</tr>
<tr>
<td>ABOUT NAC/ARP ENFORCEMENT TECHNOLOGY</td>
<td>85</td>
</tr>
<tr>
<td>ENHANCED PROTECTION WITH KASPERSKY SECURITY NETWORK</td>
<td>86</td>
</tr>
<tr>
<td>INFORMATION ABOUT THIRD-PARTY CODE</td>
<td>87</td>
</tr>
<tr>
<td>TRADEMARK NOTICE</td>
<td>88</td>
</tr>
<tr>
<td>INDEX</td>
<td>89</td>
</tr>
</tbody>
</table>
ABOUT THIS GUIDE

This document is the Implementation Guide for Kaspersky Security Center 10 (hereinafter referred to as Kaspersky Security Center).

This Guide is intended for technical specialists tasked with installing and administering Kaspersky Security Center and supporting companies that use Kaspersky Security Center.

This guide is intended to:

- Provide a general description of Kaspersky Security Center operating principles, system requirements, standard deployment scenarios, and particularities of integration with other applications.
- Help plan the deployment of Kaspersky Security Center in an enterprise network.
- Describe the preparation for Kaspersky Security Center installation, the application installation and activation process.
- Give Kaspersky Security Center support and administration advice after installation.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

- In this document .......................................................... 6
- Document conventions .................................................. 8

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 9)

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

Kaspersky Security Center (see page 11)

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

Application architecture (see page 12)

This section describes Kaspersky Security Center and the logic of their interaction.

Hardware and software requirements (see page 13)

This section describes the hardware and software requirements for the network computers.

Administration Server performance details (see page 16)

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

Standard deployment schemes of anti-virus protection (see page 18)

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 19)

This section describes processes of protection system deployment within an enterprise that correspond to the standard deployment schemes.
Deploying a protection system in a client organization's network (see page 21)
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 24)
This section describes stages of Administration Server deployment.

Configuring a protection system in a client organization's network (see page 42)
This section describes the features of setup of a protection system using Administration Console on a client enterprise network.

Remote installation of applications (see page 45)
This section describes ways of installing and uninstalling Kaspersky Lab applications remotely.

Local installation of applications (see page 57)
This section provides an installation procedure for applications that can be installed on a local computer only.

Connecting mobile devices to Administration Server (see page 61)
This section describes how to connect to Administration Server mobile devices supporting Exchange ActiveSync® and iOS Mobile Device Management (iOS MDM) protocols.

Configuring SMS delivery in Kaspersky Security Center (see page 70)
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 workload (see page 72)
This section contains information about the volume of network traffic that the client computers and the Administration Server exchange during key administrative operations.

Speed rate for filling up the Administration Server database with events (see page 76)
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 77)
This section explains how to contact Technical Support Service.

Glossary
This section lists terms used in the guide.

Kaspersky Lab ZAO (see page 84)
This section provides information about Kaspersky Lab.

Information about third-party code (see page 87)
This section provides information about third-party code used in Kaspersky Security Center.

Trademark notice (see page 88)
This section contains registered trademark notices.

Index
This section helps you find necessary data quickly.
DOCUMENT CONVENTIONS

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

<table>
<thead>
<tr>
<th>SAMPLE TEXT</th>
<th>DOCUMENT CONVENTIONS DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that...</td>
<td>Warnings are highlighted with red color and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.</td>
</tr>
<tr>
<td>We recommend that you use...</td>
<td>Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.</td>
</tr>
<tr>
<td><strong>Example:</strong> ...</td>
<td>Examples are given on a yellow background under the heading &quot;Example&quot;.</td>
</tr>
<tr>
<td>Update means...</td>
<td>The following semantic elements are italicized in the text:</td>
</tr>
<tr>
<td>The Databases are out of date event occurs.</td>
<td>• new terms;</td>
</tr>
<tr>
<td>Press ENTER. Press ALT+F4.</td>
<td>Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys should be pressed simultaneously.</td>
</tr>
<tr>
<td>Click the Enable button.</td>
<td>Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.</td>
</tr>
<tr>
<td>➤ To configure task schedule:</td>
<td>Introductory phrases of instructions are italicized and accompanied by the arrow sign.</td>
</tr>
<tr>
<td>Enter help in the command line</td>
<td>The following types of text content are set off with a special font:</td>
</tr>
<tr>
<td>The following message then appears:</td>
<td>• text in the command line;</td>
</tr>
<tr>
<td>Specify the date in dd:mm:yy format.</td>
<td>• text of messages displayed on the screen by the application;</td>
</tr>
<tr>
<td>&lt;User name&gt;</td>
<td>Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.</td>
</tr>
</tbody>
</table>
SOURCES OF INFORMATION ABOUT THE APPLICATION

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

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

In this section:

Sources of information for independent research ................................................................. 9
Discussing Kaspersky Lab applications on the forum ........................................................... 10
Contacting the Technical Writing and Localization Unit ....................................................... 10

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to find information about the application:

- the application's page at the Kaspersky Lab website;
- the application's Knowledge Base page at the Technical Support Service website;
- online help;
- documentation.

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page 77).

To use information sources on the Kaspersky Lab website, an Internet connection should be established.

Application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

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

The page http://www.kaspersky.com contains a link to the eStore. There you can purchase or renew the application.

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. Knowledge Base comprises reference articles grouped by topics.

On the page of the application in the Knowledge Base (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.

Articles may provide answers to questions that are out of scope of Kaspersky Security Center, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

Online help

The online help of the application comprises help files.

The context help provides details on each of the windows of the application: a list of settings with respective descriptions, as well as links to tasks where those settings are applied.

Full help provides information about managing computer protection, configuring the application and solving typical user tasks.
Documentation

The distribution kit includes documents that help you to install and activate the application on the computers of a local area network, configure its settings, and find information about the basic techniques for using the application.

**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.

**CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT**

If you have any questions about the documentation, please contact our Technical Documentation Development Group. For example, if you would like to leave feedback.
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 access to detailed information about the organization’s network security level; it allows configuring all the components of protection built using Kaspersky Lab applications.

Kaspersky Security Center is an application aimed at corporate network administrators and employees responsible for anti-virus protection in organizations.

The SPE version of the application is designed for SaaS providers (hereinafter referred to as service provider).

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 computers 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 computers over the network, as well as performing remote installation of applications by Kaspersky Lab and other software vendors.
- Perform remote administration of applications by Kaspersky Lab and other vendors installed on client computers. 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.
- Control access of devices to an organization’s network using access restriction rules and a white list of devices. NAC agents are used to manage access of devices to an organization’s network.
- Manage mobile devices that support Exchange ActiveSync® or iOS Mobile Device Management (iOS MDM) protocols.
- Manage encryption of information stored on the hard drives of devices and removable media 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 anti-virus applications, as well as objects for which processing by anti-virus applications has been postponed.
APPLICATION ARCHITECTURE

This section describes Kaspersky Security Center and the logic of 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 devices server**. Provides access to mobile devices and allows managing them through Administration Console. The mobile devices server collects information about mobile devices and stores their profiles.

- **Kaspersky Security Center 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

This section describes the hardware and software requirements for the network computers.

Administration Server and Kaspersky Security Center Web-Console

Table 2. Software requirements for Administration Server and Kaspersky Security Center Web-Console

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows XP Professional with Update Package 2 or later installed; Microsoft Windows XP Professional x64 or later; Microsoft Windows Vista® Business / Enterprise / Ultimate Service Pack 1 or later; Microsoft Windows Vista Business / Enterprise / Ultimate x64 Service Pack 1 or later; Microsoft Windows 7 Professional / Enterprise / Ultimate; Microsoft Windows 7 Professional / Enterprise / Ultimate x64; Microsoft Windows 8 (all editions); Microsoft Windows 8 x64 (all editions); Microsoft Windows Small Business Server 2003; Microsoft Windows Small Business Server 2008; Microsoft Windows Small Business Server 2011; Microsoft Windows Server® 2003 or later; Microsoft Windows Server 2003 x64 or later; Microsoft Windows Server 2008; Microsoft Windows Server 2008 deployed in the Server Core mode; Microsoft Windows Server 2008 x64 Service Pack 1 or later; Microsoft Windows Server 2008 x64 deployed in the Server Core mode; Microsoft Windows Server 2008 R2; Microsoft Windows Server 2008 R2 deployed in the Server Core mode; Microsoft Windows Server 2012 (all editions); Microsoft Windows Server 2012 deployed in the Server Core mode.</td>
</tr>
<tr>
<td>Data Access Components</td>
<td>Microsoft Data Access Components (MDAC) 2.8 or later Microsoft Windows DAC 6.0.</td>
</tr>
<tr>
<td>Database Management System</td>
<td>Microsoft SQL Server® Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2008 R2, Microsoft SQL Server Express 2008 R2 with Service Pack 2 installed, Microsoft SQL Server Express 2012; Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012; MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.0.87 Service Pack 1, 5.0.91; MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.</td>
</tr>
<tr>
<td>Web server</td>
<td>Apache HTTP Server version 2.2.0 or later (version 2.2.23 recommended).</td>
</tr>
</tbody>
</table>

Table 3. Hardware requirements for Administration Server and Kaspersky Security Center Web-Console

<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>CPU FREQUENCY, GHZ</th>
<th>RAM SIZE, GB</th>
<th>AVAILABLE DISK SPACE, GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows, 32-bit</td>
<td>1 or higher</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Microsoft Windows, 64-bit</td>
<td>1.4 or higher</td>
<td>4</td>
<td>10</td>
</tr>
</tbody>
</table>
Administration Console

**Table 4. Software requirements to Administration Console**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows (supported version of the operating system is determined by the requirements of Administration Server).</td>
</tr>
<tr>
<td>Management Console</td>
<td>Microsoft Management Console 2.0 or later.</td>
</tr>
<tr>
<td>Browser</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table 5. Hardware requirements to Administration Console**

<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>CPU FREQUENCY, GHz</th>
<th>RAM SIZE, MB</th>
<th>AVAILABLE DISK SPACE, GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows, 32-bit</td>
<td>1 or higher</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft Windows, 64-bit</td>
<td>1.4 or higher</td>
<td>512</td>
<td>1</td>
</tr>
</tbody>
</table>

When using the System Administration, at least 100 GB free disk space shall be available.

**iOS Mobile Device Management mobile device server**

**Table 6. Software requirements to the iOS MDM mobile device server**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows (supported version of the operating system is determined by the requirements of Administration Server).</td>
</tr>
</tbody>
</table>

**Table 7. Hardware requirements to the iOS MDM mobile device server**

<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>CPU FREQUENCY, GHz</th>
<th>RAM SIZE, GB</th>
<th>AVAILABLE DISK SPACE, GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows, 32-bit</td>
<td>1 or higher</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft Windows, 64-bit</td>
<td>1.4 or higher</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Exchange ActiveSync mobile device server**

All software and hardware requirements for Exchange ActiveSync Mobile devices server are included in requirements for the Microsoft Exchange Server.


**Network Agent or Update Agent**

**Table 8. Software requirements to Network Agent and Update Agent**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows; Linux®; Mac OS</td>
</tr>
</tbody>
</table>

The version of the operating system supported is defined by the requirements of applications that can be managed using Kaspersky Security Center.
### Hardware and Software Requirements

#### Table 9. Hardware requirements to Network Agent and Update Agent

<table>
<thead>
<tr>
<th>Operating System</th>
<th>CPU Frequency, GHz</th>
<th>RAM Size, GB</th>
<th>Free Disk Space Available for the Administration Agent, GB</th>
<th>Free Disk Space Available for Update Agent, GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows, 32-bit</td>
<td>1 or higher</td>
<td>0.5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Microsoft Windows, 64-bit</td>
<td>1.4 or higher</td>
<td>0.5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Linux, 32-bit</td>
<td>1 or higher</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Linux, 64-bit</td>
<td>1.4 or higher</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Mac OS</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

For concurrent installation of Network Agent and Kaspersky Endpoint Security, free disk space must be at least 2 GB.

You can retrieve details of the latest version of the hardware and software requirements from Technical Support website, on the page of Kaspersky Security Center 10, in the System requirements section.
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 have allowed defining maximum numbers of client computers with which Administration Server can be synchronized for specified time periods. This information can be used to identify the optimum scheme for implementation of anti-virus protection on a corporate network.

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

- 32-bit operating system (dual-core Intel® Core®2 Duo E8400 with operating frequency 3.00 GHz, 4 GB RAM, HDD SATA 500 GB);
- 64-bit operating system (4-core processor Intel Xeon® E5450 with operating frequency 3.00 GHz, 8 GB RAM, HDD SAS 2x320 RAID 0).

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

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

<table>
<thead>
<tr>
<th>Table 10. Summarized results of Administration Server performance testing under a 32-bit operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization interval (min)</td>
</tr>
<tr>
<td>--------------------------------</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>30</td>
</tr>
<tr>
<td>45</td>
</tr>
<tr>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 11. Summarized results of Administration Server performance testing under a 64-bit operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization interval (min)</td>
</tr>
<tr>
<td>--------------------------------</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>30</td>
</tr>
<tr>
<td>45</td>
</tr>
<tr>
<td>60</td>
</tr>
</tbody>
</table>

If you connect Administration Server to a MySQL or SQL Express database server, it is not recommended to use the application to manage more than 5,000 computers.
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, the distribution of anti-virus databases and modification of policies for client computers.

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 computers 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 computers.

3. Analyze information from (1) and (2), as well as data from loading tests of the administration system (see the section "Network load" on page 72). 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 computers are connected to a single Administration Server. Administration Server functions as Update Agent.
- One Administration Server with Update Agents. All client computers are connected to a single Administration Server. Some of the networked client computers function as Update Agents.
- Hierarchy of Administration Servers. 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 computers function 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.

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:
  - by using the Administration Console
  - by using Kaspersky Security Center Web-Console.

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

  The basic deployment scheme is protection system deployment via Administration Console. Using Kaspersky Security Center Web-Console allows starting installation of Kaspersky Lab applications from a browser.

- Deploying a protection system manually using standalone installation packages created in Kaspersky Security Center.

  Installation of Kaspersky Lab applications on client computers and the administrator's workstation is performed manually; the settings for connection of client computers to the Administration Server are specified when installing Network Agent.

  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 ........................................ 19
Deploying a protection system using Kaspersky Security Center Web-Console within an organization .................................................. 19
Deploying a protection system manually within an organization ........................................................................... 20

DEPLOYING A PROTECTION SYSTEM USING 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 to a selected computer;
   b. installs the Administration Console on the administrator's workstation (if necessary);
   c. adjusts the Administration Server settings.

2. If necessary, the administrator creates Administration Server hierarchy.

3. The administrator creates a structure of administration groups and distributes client computers 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 the Administration Console the administrator selects computers to which they want to install the required applications.

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 WEB-CONSOLE WITHIN AN ORGANIZATION

Remote installation of required software via Kaspersky Security Center Web-Console 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 to a selected computer;
Manual installation of required software with standalone 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 to a selected computer;
   b. installs the Administration Console on the administrator's workstation (if necessary);
   c. adjusts the Administration Server settings.
2. If necessary, the administrator creates Administration Server hierarchy.
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 the client computers by, for example, publishing a link to the installation packages.
7. Users of the client computers start installation of applications by using the stand-alone installation packages received.
8. After the client computers are connected to the Administration Server, they are moved to the respective administration groups specified in the properties of the respective 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 .................................................. 21
Deploying a protection system using Kaspersky Security Center Web-Console in a client organization's network ........ 22
Deploying a protection system on a client organization's network manually ........................................................................... 22

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 to a selected computer;
   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator's workstation (if necessary);
   d. configures Administration Server for work with Kaspersky Security Center Web-Console.

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

3. The administrator of Kaspersky Security Center selects a computer on the organization's network that should act as Update Agent, and installs Network Agent to it locally.
   As a result, Kaspersky Security Center automatically appoints the client computer on which the Network Agent is installed as the Update Agent and configures it as a connection gateway at the first connection to 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 administrator of Kaspersky Security Center selects computers to which the selected applications should 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 WEB-CONSOLE IN A CLIENT ORGANIZATION’S NETWORK

Remote installation of required software via Kaspersky Security Center Web-Console 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 to a selected computer;
   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator’s workstation (if necessary);
   d. configures Administration Server for work with Kaspersky Security Center Web-Console.

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

3. The administrator selects a computer on the network that should act as Update Agent, and installs the Network Agent on it locally.

As a result, Kaspersky Security Center automatically appoints the client computer on which the Network Agent is installed as the Update Agent and configures it as a connection gateway at the first connection to 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 Web-Console the client enterprise administrator starts installation of selected applications on client computers.

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 standalone 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 to a selected computer;
   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator’s workstation (if necessary);
   d. configures Administration Server for work with Kaspersky Security Center Web-Console.

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

3. The administrator selects a computer on the network that should act as Update Agent, and installs the Network Agent on it locally.

As a result, Kaspersky Security Center automatically appoints the client computer on which the Network Agent is installed as the Update Agent and configures it as a connection gateway at the first connection to 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 standalone installation packages for selected applications.

6. Kaspersky Security Center administrator sends the standalone installation package to their client organization (for example, by publishing the link to the package in Kaspersky Security Center Web-Console).

7. The administrator of the client organization sends the standalone package to the selected computers through Kaspersky Security Center Web-Console.

8. Users of client computers start application installation by using a standalone installation package.

9. After the client computer is connected to Administration Server, it is moved to administration group specified the properties of the stand-alone package.
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 (when using the SPE version of the application).

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

Kaspersky Security Center supports integration with the Microsoft Network Access Protection (NAP) that allows managing client computer access to network. To ensure checking of the operating system’s operability when running Kaspersky Security Center concurrently with Microsoft NAP, you should additionally install the System Health Validator component (see the section “Installing and configuring Kaspersky Security Center SHV” on page 37).

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

### In this section:

<table>
<thead>
<tr>
<th>Stages of deploying Administration Server within an enterprise</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steps of Administration Server deployment for protection of a client organization's network</td>
<td>24</td>
</tr>
<tr>
<td>Upgrading the previous version of Kaspersky Security Center</td>
<td>25</td>
</tr>
<tr>
<td>Installing and removing Kaspersky Security Center</td>
<td>25</td>
</tr>
<tr>
<td>Installing Administration Console on the administrator's workstation</td>
<td>37</td>
</tr>
<tr>
<td>Installing and configuring Kaspersky Security Center SHV</td>
<td>37</td>
</tr>
<tr>
<td>Installing Kaspersky Security Center Web-Console</td>
<td>38</td>
</tr>
<tr>
<td>Configuring interaction between Administration Server and Kaspersky Security Center Web-Console</td>
<td>40</td>
</tr>
</tbody>
</table>

### 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 Web-Console on the administrator's workstation.
UPGRADING THE PREVIOUS VERSION OF KASPERSKY SECURITY CENTER

You can install Administration Server 10 to a computer where the previous version of Administration Server is installed. When you upgrade Administration Server to version 10, all data and settings from the previous version of the application are saved.

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

1. Run the executable file setup.exe for the version 10.
   The Setup Wizard starts. Follow the wizard's instructions.

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 data copy 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 Creating Administration Server backup copy window that opens, select the Create Administration Server backup copy 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.

Cancelling the product setup at an installation stage of Administration Server can cause Kaspersky Security Center 9.0 to fail.

5. For computers where a previous version of Network Agent has been installed, create and run the remote installation task for the new version of Network Agent (see the section "Installing applications using the remote installation task" on page 46).
   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 deployment 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 installation: 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 computers.
- 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 computers. Custom installation is recommended for experienced users.

If at least one Administration Server is installed in the network, Servers can be installed to other computers remotely through the remote installation task using push installation (see the section "Installing applications using a remote installation task" on page 46). When creating the remote installation task, you should use the Administration Server installation package.
In this section:

Preparing for installation ................................................................. 26
Typical installation ........................................................................... 27
Custom installation ........................................................................... 28
Installation in non-interactive mode .................................................. 33
Changes in the system after installing the application ......................... 35
Removing the application ................................................................. 37

Preparing for installation

Before starting the setup process, make sure that the hardware and software of the host computer meet the requirements for Administration Server and Administration Console (see the section “Hardware and software requirements” on page 13).

Kaspersky Security Center stores its information in a SQL Server database. Therefore, by default, Microsoft SQL Server 2008 R2 Express Edition is installed together with Kaspersky Security Center. Other SQL Servers can also be used for data storage (see the section “Hardware and software requirements” on page 13). In that case they must be installed on the network before the start of installation of Kaspersky Security Center.

Installation of Kaspersky Security Center requires administrator privileges on the computer on which the installation is performed.

To ensure that application components function correctly after setup, all the required ports must be open on the host computers (see the following table).

<table>
<thead>
<tr>
<th>PORT NUMBER</th>
<th>PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer on which Administration Server is installed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8060</td>
<td>HTTP</td>
<td>Used for connecting to Web Server for access to Kaspersky Security Center Web-Console and administering the enterprise’s intranet.</td>
</tr>
<tr>
<td>8061</td>
<td>HTTPS</td>
<td>Used for connecting to Web Server for access to Kaspersky Security Center Web-Console and administering the enterprise’s intranet. This connection type uses encryption.</td>
</tr>
</tbody>
</table>
| 13000       | TCP      | Used to:  
- Retrieve data from client computers  
- Connect to Update Agents  
- Connect to slave Administration Servers  
SSL protection is used for these connections. |
| 13000       | UDP      | Used to transfer information if a computer is shut down. |
| 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. |
| 14000       | TCP      | Used to:  
- Retrieve data from client computers  
- Connect to Update Agents  
- Connect to slave Administration Servers  
SSL protection is not used for these connections. |
### Deploying Administration Server

<table>
<thead>
<tr>
<th>PORT NUMBER</th>
<th>PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>17000</td>
<td>TCP</td>
<td>Used for connecting to an activation proxy server. SSL protection is used for these connections.</td>
</tr>
<tr>
<td>17100</td>
<td>TCP</td>
<td>Used for connecting to an activation proxy server in order to activate mobile clients.</td>
</tr>
<tr>
<td>18000</td>
<td>HTTP</td>
<td>Administration Server uses this port to receive data from a Cisco® NAC authentication server.</td>
</tr>
</tbody>
</table>

**Computer designated as Update Agent**

<table>
<thead>
<tr>
<th>PORT NUMBER</th>
<th>PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>13000</td>
<td>TCP</td>
<td>The port is used by client computers to connect to the Update Agent.</td>
</tr>
<tr>
<td>13001</td>
<td>TCP</td>
<td>The port is used by client computers to connect to the Update Agent if a computer with Administration Server installed functions as an Update Agent.</td>
</tr>
<tr>
<td>14000</td>
<td>TCP</td>
<td>The port is used by client computers to connect to the Update Agent.</td>
</tr>
<tr>
<td>14001</td>
<td>TCP</td>
<td>The port is used by client computers to connect to the Update Agent if a computer with Administration Server installed functions as an Update Agent.</td>
</tr>
</tbody>
</table>

**Client computer with Network Agent installed**

<table>
<thead>
<tr>
<th>PORT NUMBER</th>
<th>PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>UDP</td>
<td>The port is used by the Wake On LAN feature.</td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>Used on a computer that has been assigned to be the PXE server when deploying operating system images.</td>
</tr>
<tr>
<td>69</td>
<td>UDP</td>
<td>The port is used to receive requests for connection to the Administration Server, which can collect information about a host computer in real time.</td>
</tr>
<tr>
<td>15,000</td>
<td>UDP</td>
<td>Used to interact with Update Agent.</td>
</tr>
</tbody>
</table>

For outbound connections of client computers to the Administration Server and Update Agents, the range of ports 1024–5000 (TCP) is used. In Microsoft Windows Vista and Microsoft Windows Server2008 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 computer:

1. Run the file setup.exe. The Setup Wizard prompts you to configure application settings. Follow the wizard’s instructions.

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 **Typical** and click the **Next** button.

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

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
- Available management plug-ins for applications.

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

- Microsoft Windows Installer 3.1
- Microsoft Data Access Component 2.8
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2008 R2 Express Edition

CUSTOM INSTALLATION

To perform custom installation of Kaspersky Security Center on a local computer:

Run the file setup.exe.

This starts the Setup Wizard. Follow the wizard’s instructions.

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

THE WIZARD’S STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Reviewing the License Agreement</td>
</tr>
<tr>
<td>2.</td>
<td>Selecting an installation method</td>
</tr>
<tr>
<td>3.</td>
<td>Selecting the components to be installed</td>
</tr>
<tr>
<td>4.</td>
<td>Selecting network size</td>
</tr>
<tr>
<td>5.</td>
<td>Selecting an account</td>
</tr>
<tr>
<td>6.</td>
<td>Selecting a database</td>
</tr>
<tr>
<td>7.</td>
<td>Configuring SQL Server</td>
</tr>
<tr>
<td>8.</td>
<td>Selecting an authentication mode</td>
</tr>
<tr>
<td>9.</td>
<td>Selecting a shared folder</td>
</tr>
<tr>
<td>10.</td>
<td>Configuring the connection to Administration Server</td>
</tr>
<tr>
<td>11.</td>
<td>Defining the Administration Server address</td>
</tr>
<tr>
<td>12.</td>
<td>Configuring settings for mobile devices</td>
</tr>
<tr>
<td>13.</td>
<td>Selecting application management plug-ins</td>
</tr>
<tr>
<td>14.</td>
<td>Completing installation</td>
</tr>
</tbody>
</table>

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 End User License Agreement check box. Installation then proceeds.

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:

- **Kaspersky Lab Cisco NAC Posture Validation Server** This is a standard Kaspersky Lab component that authorizes a set of credentials for interfacing with Cisco® NAC. The settings for interaction with Cisco® NAC can be configured in the Administration Server properties or policy (for details, please see the Kaspersky Security Center Administrator’s Guide).

- **Mobile devices support.** This component ensures management of mobile device protection through Kaspersky Security Center.

- **SNMP agent.** This component supports collection of statistical information for the Administration Server over the SNMP protocol. The component is available if the application is installed on a computer that has SNMP installed.

After Kaspersky Security Center is installed, the .mib files required for collecting statistical data are located in the SNMP subfolder of the installation folder of the application.

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 computer 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 computer, remove it and start installation of Administration Server 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 computers on the network, the Wizard configures installation and appearance of the application interface to match.

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

<table>
<thead>
<tr>
<th>Settings</th>
<th>1 to 100 Computers</th>
<th>100 to 1,000 Computers</th>
<th>1,000 to 5,000 Computers</th>
<th>5,000+ Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display of node for slave and virtual Administration Servers and all settings related to slave and virtual Administration Servers in the console tree</td>
<td>not available</td>
<td>not available</td>
<td>available</td>
<td>available</td>
</tr>
<tr>
<td>Display of <strong>Security</strong> sections in the properties windows of the Administration Server and administration groups</td>
<td>not available</td>
<td>not available</td>
<td>available</td>
<td>available</td>
</tr>
</tbody>
</table>
**STEP 5. SELECTING AN ACCOUNT**

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

- **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.** Administration Server will start under the selected user’s account. Administration Server will initiate all operations by using the credentials of that account. To select the user whose account will be used, click the **Browse** button and enter the user's password.

When using an SQL server in a mode that uses Microsoft Windows tools for authenticating user accounts, access to the database should be granted. The user 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. 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 7. 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 name of an SQL Server appears in the **SQL Server name** field by default if it is detected on the computer on which Kaspersky Security Center is being 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 plan to manage fewer than 5,000 computers with Kaspersky Security Center, Microsoft SQL Express 2005 / 2008 can be used. If the planned number of computers to be managed with Kaspersky Security Center exceeds 5,000, Microsoft SQL 2005 / 2008 is recommended.

- If SQL Server is not installed on the network, select the option **Install Microsoft SQL Server 2008 R2 Express Edition**.
  
The Setup Wizard then installs Microsoft SQL Server 2008 R2 Express Edition. The necessary settings are configured automatically.

- If a MySQL Server was selected during the previous step, use this window to specify its name in the **SQL Server name** field (by default, the system uses the IP address of the computer on which Kaspersky Security Center is being 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 an SQL Server manually on the computer from which you are initiating installation of Kaspersky Security Center, you must terminate installation and restart it after installation of SQL Server. The supported SQL Servers are listed in the system requirements (see the section "Hardware and software requirements" on page 13). If you are installing the server on a remote computer, there is no need to interrupt the Kaspersky Security Center Setup Wizard. Install SQL Server and return to installation of Kaspersky Security Center.

**STEP 8. 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 stored on another computer and the Administration Server account has no access to the database server, you must use SQL Server authentication mode when installing or upgrading Administration Server. This may occur when the computer 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 9. 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 deployment 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 computer that is used for installation or a remote directory on any client computer on 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\KLSHARE) in the corresponding field.

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

**STEP 10. 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 over the 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 computer after installation, these ports must be opened manually.

**STEP 11. DEFINING THE ADMINISTRATION SERVER ADDRESS**

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

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

When installing the SPE version of the application, it is recommended to use a DNS name or an IP address as the Administration Server address. When you create a virtual Administration Server, the address specified during this wizard step is used as the default master Administration Server address.

**STEP 12. CONFIGURING SETTINGS FOR MOBILE DEVICES**

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

Specify the Administration Server address for mobile device connections.

When installing the SPE version of the application, it is recommended to use a DNS name or an IP address as the Administration Server address. When you create a virtual Administration Server, the address specified during this wizard step is used as the default master Administration Server address.

**STEP 13. SELECTING APPLICATION MANAGEMENT PLUG-INS**

Select the application management plug-ins that you want to install with Kaspersky Security Center.

**STEP 14. COMPLETING INSTALLATION**

After installation of Kaspersky Security Center components is configured, you can start the installation process.

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 to a local computer 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).

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 14. Settings of Administration Server installation in non-interactive mode

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Setting Description</th>
<th>Available Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>EULA</td>
<td>Acceptance of the terms of the License Agreement</td>
<td>• 1 – I accept the terms of the License Agreement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• other value, or no value – I do not accept the terms of the License Agreement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(no installation will be performed)</td>
</tr>
<tr>
<td>INSTALLATIONMODETYPE</td>
<td>Type of Administration Server installation</td>
<td>• Standard – standard installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom – custom installation</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td>Path to the Administration Server installation folder</td>
<td>String value</td>
</tr>
<tr>
<td>ADDLOCAL</td>
<td>List of Administration Server components (separated with commas) to be installed</td>
<td>CSAdminKitServer, Nagent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CiscoNacServer, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86</td>
</tr>
<tr>
<td>NETRANGETYPE</td>
<td>Network size (number of computers on the network)</td>
<td>• NRT_1_100 – from 1 to 100 computers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NRT_100_1000 – from 100 to 1,000 computers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NRT_GREATER_1000 – 1,000 or more computers</td>
</tr>
<tr>
<td>SRV_ACCOUNT_TYPE</td>
<td>Mode for specifying the account under which Administration Server will be run as a service</td>
<td>• SrvAccountDefault – the account is created automatically</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SrvAccountUser – the account is created manually; in this case, you must</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specify values for the SERVERACCOUNTNAME and SERVERACCOUNTPWD settings</td>
</tr>
<tr>
<td>SERVERACCOUNTNAME</td>
<td>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</td>
<td>String value</td>
</tr>
<tr>
<td>SERVERACCOUNTPWD</td>
<td>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</td>
<td>String value</td>
</tr>
<tr>
<td><strong>SETTING NAME</strong></td>
<td><strong>SETTING DESCRIPTION</strong></td>
<td><strong>AVAILABLE VALUES</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBTYPE</td>
<td>Type of database that will be created to store the Administration Server database.</td>
<td>• MySQL – MySQL database will be used; in this case, you must specify values for the MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME, and MYSQLACCOUNTPWD settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MSSQL – Microsoft SQL Server (SQL Express) database will be used; in this case, you must specify values for the MSSQLCONNECTIONTYPE and MSSQLAUTHTYPE settings</td>
</tr>
<tr>
<td>MYSQLSERVERNAME</td>
<td>Full name of the SQL server; you must specify a value for the setting if DBTYPE=MySQL</td>
<td>String value</td>
</tr>
<tr>
<td>MYSQLSERVERPORT</td>
<td>Number of the port for connecting to the SQL server; you must specify a value for the setting if DBTYPE=MySQL</td>
<td>String value</td>
</tr>
<tr>
<td>MYSQLDBNAME</td>
<td>Name of the database that will be created to store Administration Server data; you must specify a value for the setting if DBTYPE=MySQL</td>
<td>String value</td>
</tr>
<tr>
<td>MYSQLACCOUNTNAME</td>
<td>Name of the account for connecting to the database; you must specify a value for the setting if DBTYPE=MySQL</td>
<td>String value</td>
</tr>
<tr>
<td>MYSQLACCOUNTPWD</td>
<td>Password of the account for connecting to the database; you must specify a value for the setting if DBTYPE=MySQL</td>
<td>String value</td>
</tr>
<tr>
<td>MSSQLCONNECTIONTYPE</td>
<td>Type of use of the MSSQL database; you must specify a value for the setting if DBTYPE=MSSQL</td>
<td>• InstallMSSEE – install Microsoft SQL Server 2008 R2 Express Edition; all the required settings will be defined automatically</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ChooseExisting – use an SQL server installed on the enterprise network; in this case, you must specify values for the MSSQLSERVERNAME and MSSQLDBNAME settings</td>
</tr>
<tr>
<td>MSSQLSERVERNAME</td>
<td>Full name of the SQL server; you must specify a value for the setting if MSSQLCONNECTIONTYPE=ChooseExisting</td>
<td>String value</td>
</tr>
<tr>
<td>MSSQLDBNAME</td>
<td>Name of the database; you must specify a value for the setting if MSSQLCONNECTIONTYPE=ChooseExisting</td>
<td>String value</td>
</tr>
<tr>
<td>MSSQLAUTHTYPE</td>
<td>Type of authorization when connecting to the SQL server; you must specify a value for the setting if DBTYPE=MSSQL</td>
<td>• Windows – Microsoft Windows authentication mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SQLServer – SQL server authentication mode; in this case, you must specify values for the MSSQLACCOUNTNAME and MSSQLACCOUNTPWD settings</td>
</tr>
<tr>
<td>MSSQLACCOUNTNAME</td>
<td>Name of the account for connection to the SQL server; you must specify a value for the setting if MSSQLAUTHTYPE=SQLServer</td>
<td>String value</td>
</tr>
</tbody>
</table>
## Deploying Administration Server

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Setting Description</th>
<th>Available Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSSQLACCOUNTPWD</td>
<td>Password of the account for connection to the SQL server; you must specify a value for the setting if MSSQLAUTHTYPE=SQLServer</td>
<td>String value</td>
</tr>
<tr>
<td>CREATE_SHARE_TYPE</td>
<td>Method of specifying a shared folder</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Create – create a new shared folder; in this case, you must specify values for the SHARELOCALPATH and SHAREFOLDERNAME settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ChooseExisting – select an existing folder; in this case, you must specify a value for the EXISTSHAREFOLDERNAME setting</td>
<td></td>
</tr>
<tr>
<td>SHARELOCALPATH</td>
<td>Full path to a local folder; you must specify a value for the setting if CREATE_SHARE_TYPE=Create</td>
<td>String value</td>
</tr>
<tr>
<td>SHAREFOLDERNAME</td>
<td>Network name of a shared folder; you must specify a value for the setting if CREATE_SHARE_TYPE=Create</td>
<td>String value</td>
</tr>
<tr>
<td>EXISTSHAREFOLDERNAME</td>
<td>Full path to an existing shared folder; you must specify a value for the setting if CREATE_SHARE_TYPE=ChooseExisting</td>
<td>String value</td>
</tr>
<tr>
<td>SERVERPORT</td>
<td>The port number to connect to the Administration Server</td>
<td>Numerical value</td>
</tr>
<tr>
<td>SERVERSSLPORT</td>
<td>Port number to connect to Administration Server by using SSL protocol</td>
<td>Numerical value</td>
</tr>
<tr>
<td>SERVERADDRESS</td>
<td>Administration Server address</td>
<td>String value</td>
</tr>
<tr>
<td>MOBILESERVERADDRESS</td>
<td>Administration Server address for connections with mobile devices</td>
<td>String value</td>
</tr>
</tbody>
</table>

**Example of a command for installation of Administration Server in non-interactive mode:**

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

For a detailed description of Administration Server installation settings please refer to the "Custom installation".

## Changes in the System after Installing the Application

After Administration Console is installed on your computer, 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 computer as services with the properties listed below. The table also contains the attributes of other services that apply on the computer after Administration Server installation.

The Kaspersky Lab Posture Validation Server service for Cisco® NAC is applied on the computer if the Kaspersky Lab Cisco® NAC Posture Validation Server has been installed together with Administration Server.
Table 15. Service attributes

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>SERVICE NAME</th>
<th>DISPLAYED SERVICE NAME</th>
<th>STARTUP TYPE</th>
<th>ACCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Server</td>
<td>kladminserver</td>
<td>Kaspersky Security Center Administration Server</td>
<td>Automatically when the operating system starts up</td>
<td>User-defined or dedicated account (of the format KL-AK-*, created during installation)</td>
</tr>
<tr>
<td>Kaspersky Lab Cisco NAC Posture Validation Server</td>
<td>klnacserver</td>
<td>Kaspersky Lab Cisco NAC Posture Validation Server</td>
<td>Automatically when the operating system starts up</td>
<td>Local system</td>
</tr>
<tr>
<td>Network Agent</td>
<td>klnagent</td>
<td>Kaspersky Security Center Network Agent</td>
<td>Automatically when the operating system starts up</td>
<td>Local system</td>
</tr>
<tr>
<td>Web server for accessing Web-Console and administering the enterprise's intranet</td>
<td>klwebsrv</td>
<td>Kaspersky Lab web server</td>
<td>Automatically when the operating system starts up</td>
<td>Dedicated unprivileged account in KlScSvc-* format</td>
</tr>
<tr>
<td>Activation proxy server</td>
<td>klactprx</td>
<td>Kaspersky Lab's activation proxy server</td>
<td>Automatically when the operating system starts up</td>
<td>Dedicated unprivileged account in KlScSvc-* format</td>
</tr>
<tr>
<td>Access authorization web portal</td>
<td>klnsacwsrv</td>
<td>Kaspersky Lab's authorization portal</td>
<td>Manually</td>
<td>Local system</td>
</tr>
<tr>
<td>KSN proxy server</td>
<td>ksnproxy</td>
<td>Kaspersky Security Network proxy server</td>
<td>Manually</td>
<td>Dedicated unprivileged account in KlScSvc-* format</td>
</tr>
<tr>
<td>iOS MDM server</td>
<td>KLIOSMdmServiceSrv2</td>
<td>iOS MDM Mobile devices server</td>
<td>Automatically when the operating system starts up</td>
<td>Network Service</td>
</tr>
<tr>
<td>COM+ object for interaction with Exchange server</td>
<td>KasperskyMdmService</td>
<td>Kaspersky MDM for Exchange</td>
<td>Automatically when calling object</td>
<td>User account included in the Domain User and KLMDM Role Group (KLMDM Secure Group) groups</td>
</tr>
</tbody>
</table>

The server version of Network Agent will be installed on the computer 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 adjust the settings for connection of Network Agent to Administration Server: setup is software-integrated taking into account the components installed on the same computer. These connection settings also will not be available in the local settings of Network Agent on that computer. 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 managed by the policy of the administration group to which the client computer of Administration Server 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.

Individual installation of Network Agent on the Administration Server computer is not required. 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 Posture Validation Server, as well as monitor their operation using standard Microsoft Windows management tools: Computer management\Services. Information about the activity of Kaspersky Lab Administration Server service is stored in the Microsoft Windows system log in a separate Kaspersky Event Log branch on the computer where the Administration Server is installed.
Local groups of users named KLAdmins and KLOperators will also be created automatically on the computer where the 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. Removing the application requires starting a wizard that removes all application components from the computer (including plug-ins). If you have not selected removal of the shared folder (KLSHARE) 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 Wizard.

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 file from the CD containing the distribution package of Kaspersky Security Center in the Console folder. This will start the Setup Wizard. Follow the wizard's instructions.

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. Start Administration Console. In the window that opens, specify the name of the computer on which Administration Server is installed and the settings of the account used to connect to it. 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.

**INSTALLING AND CONFIGURING KASPERSKY SECURITY CENTER SHV**

Kaspersky Security Center supports integration with the Microsoft Network Access Protection (NAP). Microsoft NAP allows regulation of client computer access to the network. Microsoft NAP presupposes that a server with Microsoft Windows Server 2008 is allocated on the network, and PVS (Posture Validation Server) service is installed on that server, while NAP-compatible operating systems are installed on client computers: Microsoft Windows Vista, Microsoft Windows XP Service Pack 3, and 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 to a computer locally:
1. Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center SHV. This will start the Setup Wizard. Follow the wizard's instructions.
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 will be installed on your computer.

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

**INSTALLING KASPERSKY SECURITY CENTER WEB-CONSOLE**

To install Kaspersky Security Center Web-Console to a local computer,

Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center Web-Console.

The corresponding wizard will guide you through the installation. The Setup Wizard will invite you to configure the installation settings. Follow the wizard's instructions.

The installation of Kaspersky Security Center Web-Console from the distribution package downloaded from the Internet is no different than installation from the installation CD.

**THE WIZARD’S STEPS**

1. Reviewing the License Agreement................................................................................ 38
2. Selecting the destination folder...................................................................................... 39
3. Selecting the ports........................................................................................................ 39
4. Connecting to Kaspersky Security Center..................................................................... 39
5. Selecting the Apache Server installation mode.............................................................. 39
6. Installing Apache Server.................................................................................................. 40
7. Starting installation of Kaspersky Security Center Web-Console................................. 40
8. Completing installation of Kaspersky Security Center Web-Console............................. 40

**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.

To use Kaspersky Security Center Web-Console under Linux platform, you will need a license named Kaspersky Security Center Web-Console, Service Provider Edition.

Please, read the End User License Agreement carefully. If you accept all of the provisions, select the I accept the terms of the End User License Agreement check box. Installation then proceeds.
DEPLOYING ADMINISTRATION SERVER

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

Remote installation of Kaspersky Security Center Web-Console with 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 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. SELECTING THE DESTINATION FOLDER**

Specify a destination folder for installation of Kaspersky Security Center Web-Console. 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 3. SELECTING THE PORTS**

Specify the following settings:

- **SSL port number**. Port number to connect to Administration Server by using SSL protocol. The default port number is 13291.
- **Port number**. Port number to connect the computer to Apache Server. The default port number is 9000.

**STEP 4. CONNECTING TO KASPERSKY SECURITY CENTER**

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

- **Use Apache server installed on local computer**. If this option is selected, Kaspersky Security Center Web-Console will be connected to Kaspersky Security Center via the Apache server installed on a local computer (you can select installation of Apache server at the next step of the Wizard).
- **Use Apache server installed on remote computer**. You can select this option if the Apache server is already installed on a remote computer running under Linux. In this case, only the server part of Kaspersky Security Center Web-Console will be installed. To connect Kaspersky Security Center Web-Console to Kaspersky Security Center, you should install the client part of Kaspersky Security Center Web-Console to a remote computer. If you select this option, the Setup Wizard proceeds to Step 7 (see the section "Step 7. Starting installation of Kaspersky Security Center Web-Console" on page 40).

  ➤ To install the client part of Kaspersky Security Center Web-Console on a remote computer running under 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 5. SELECTING THE APACHE SERVER INSTALLATION MODE**

If Apache Server is not installed on the computer, at this step the wizard will suggest installing Apache HTTP Server 2.2. By default, the Apache HTTP Server 2.2 installation is selected. If you do not want to install the Apache server using the Kaspersky Security Center Web-Console Setup Wizard, clear the **Install Apache HTTP Server 2.2** check box.

The Apache installation might require restarting the computer.
**STEP 6. INSTALLING APACHE SERVER**

At this step of the Setup Wizard installation and configuration of Apache HTTP Server 2.2 are performed.

Before you install Apache HTTP Server, specify the certificate for Kaspersky Security Center Web-Console to use to connect to Apache server. Select one of the following options:

- **Create new certificate.** Create a certificate for working via HTTPS.
- **Select existing certificate.** Use an existing certificate for working via HTTPS. Specify a certificate using one of the following 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.

After you have selected a certificate, click the *Next* button. This starts the Apache HTTP Server 2.2 Setup Wizard. Follow the Wizard's instructions.

**STEP 7. STARTING INSTALLATION OF KASPERSKY SECURITY CENTER WEB-CONSOLE**

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

The installation process is displayed on the Wizard page.

**STEP 8. COMPLETING INSTALLATION OF KASPERSKY SECURITY CENTER WEB-CONSOLE**

If Apache 2 Server, version 2.2.9 or later, is already installed on the computer or automatic installation of Apache 2 Server completed with an error, at the last step of the Kaspersky Security Center Web-Console Setup Wizard, you are prompted to open the file with instructions on how to configure Apache Server. To open the instructions file, select the *Open readme.txt* check box.

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

**CONFIGURING INTERACTION BETWEEN ADMINISTRATION SERVER AND KASPERSKY SECURITY CENTER WEB-CONSOLE**

*To configure the operation of the Administration Server with Kaspersky Security Center Web-Console:*

1. Place the key Kaspersky Security Center Web-Console or Kaspersky Security Center Web-Console SPE into the *Keys* folder nested into the *Storages* folder in one of the following ways:
   - using the Quick Start Wizard of the Administration Server (to start the Wizard, from the context menu of the Administration Server select *All tasks* → *Quick Start Wizard*);
   - by clicking the *Add a key* link in the *Keys* folder.
   - add the key as active one in the properties of the master Administration Server: in the properties window of the master Administration Server, in the *Keys* section, using the *Modify* button.

2. If necessary, create the Administration Server hierarchy.

3. If necessary, create the requisite virtual Administration Servers and include them in the Administration Server hierarchy.
Configure the virtual server settings as follows:

a. Select a virtual server administrator account from among the accounts offered by the application or create a new account. Under this account, the administrator of the client organization's network managed by the selected virtual Administration Server starts Kaspersky Security Center Web-Console to view details of the anti-virus security status of the network.

If necessary, you can create several accounts with administrator privileges on a virtual Server.

The administrator of a virtual Server is an internal user of Kaspersky Security Center. No data on internal users is transferred to the operating system. Kaspersky Security Center authenticates internal users.

b. Create a License Agreement file (eula.txt or eula.html) and a frequently asked questions (FAQ) file (faq.txt or faq.html).

Copy the created eula.txt (eula.html) and faq.txt (faq.html) files to the Apache server installation folder, into the nested folder htdocs\help. The links to these files are displayed in the main window of Kaspersky Security Center Web-Console.

c. Send the following information to the client organization:

- The address of the Server with pre-installed Kaspersky Security Center Web-Console (as a URL or IP address).
- Name of the virtual Administration Server that manages the whole customer network.
- User name and password of the account with administrator privileges on the virtual Administration Server.

To display the logo of your organization in the interface of Kaspersky Security Center Web-Console:

1. Prepare a logo file meeting the following requirements:
   - File format: PNG;
   - File name: logo.png;
   - File size: Any
   - Permission: 220×72 pixels.

2. Place the logo file to the installation folder of the Apache server.
   - If the Apache server has been installed under Microsoft Windows, the default path to the installation folder is as follows: C:\Program Files\Apache Software Foundation\Apache2.2\htdocs\images\custom_logo.
   - If the Apache server has been installed under Linux, the default path to the installation folder is as follows: /opt/kaspersky/kscwebconsole/share/htdocs/images/custom_logo.

For more details on how to configure Administration Server's cooperation with Kaspersky Security Center Web-Console please refer to the Kaspersky Security Center Administrator's Guide.
CONFIGURING A PROTECTION SYSTEM FOR A CLIENT ORGANIZATION'S NETWORK

This section describes the features of setup of a protection system using Administration Console on a client enterprise 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 a computer that should act as Update Agent on the network of the client enterprise.
2. Local installation of the Network Agent to Update Agent.
3. Remote installation of Network Agent and required Kaspersky Lab applications to computers of the client organization.

This section describes prerequisites for remote installation of applications to computers of a client enterprise. 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 43).

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

IN THIS SECTION:
Defining an Update Agent. Configuring Update Agent ................................................................. 42
Local installation of the Network Agent to Update Agent................................................................. 43
Requirements to installation of applications on computers of a client enterprise ................................ 44
Creating a hierarchy of administration groups subordinated to the virtual Administration Server .................. 44

DEFINING AN UPDATE AGENT. CONFIGURING UPDATE AGENT

If computers of the client organization have no direct communication with the virtual Administration Server, you can manage it via a connection gateway. The Update Agent of an administration group can act as connection gateway for the group.

To appoint a client computer as the Update Agent that should act as connection gateway for an administration group, installing the Network Agent on this computer will be enough. When this computer first connects to the Administration Server, Kaspersky Security Center automatically appoints it as the Update Agent of the group and configures it as connection gateway.

You can also select the Update Agent and configure it manually as connection gateway.

To define a computer as Update Agent:

1. In the console tree, select an administration group.
2. Open the Update Agents section in the properties window of the selected group in one of the following ways:
   • In the context menu of the administration group, select Properties. In the Properties window that opens, select the Update Agents section.
   • By clicking the Configure Update Agents for group link in the workspace of the administration group.
3. Select a computer and add it as Update Agent for the group.

To add a computer as an update agent, click the Add button and select the check box next to the name of the client computer from the Managed computers folder. You can select multiple computers at once; all of them will be added to the list.
You can choose how to add an Update Agent. Click the arrow (⋮) on the Add button. You can add computers in the following ways:

- **Add computer from group.** Adds computers from Managed computers folder.
- **Add computer by address.** Enter IP address of computer.

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

After the Update Agent is added by IP address, the Administration Server will detect it the next time it scans the network, moving it to the Unassigned computers folder. Because the Update Agent is protected by Firewall, you should perform the following actions to configure it:

1. Add this computer to the selected administration group.
2. Reopen the properties window of the selected group on the Update Agents section.
3. Remove computer that was added by address from the Update Agents list.
4. Add the same computer from the Managed computers folder by using the Add button or Add computer from group.
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.

As a result, the selected computer is appointed an Update Agent for the administration group.

---

**LOCAL INSTALLATION OF THE NETWORK AGENT TO UPDATE AGENT**

To allow the computer selected by the Update Agent to communicate the virtual Administration Server directly in order to act as connection gateway, the Network Agent should be installed locally on this computer.

The procedure of local installation of Network Agent to computer defined as Update Agent is equal to local installation of Network Agent to any network computer.

The following conditions must be met for a computer selected as an Update Agent:

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

  The following format is used for composing the address of the virtual Administration Server: `<Full address of the physical Administration Server to which the virtual Administration Server is subdued>/<Name of the virtual Administration Server>`.

- So it can perform the role of a connection gateway, open all ports of the computer that are necessary for the connection with the Administration Server.

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

- includes this computer in the Managed computers group of the virtual Administration Server.
- appoints this computer the Update Agent of the Managed computers group of the virtual Administration Server.

It is necessary and sufficient to perform local installation of the Network Agent on the computer appointed the Update Agent for the Managed computers group on the enterprise network. You can install Network Agent remotely to computers that act as Update Agents in the nested Administration Server groups. To do this, use Update Agent of the Managed computers group as connection gateway.

---

**SEE ALSO:**

- Local installation of Network Agent.................................................................................................................................57
- Remote deployment of applications........................................................................................................................................45

-
REQUIREMENTS TO INSTALLATION OF APPLICATIONS ON COMPUTERS OF A CLIENT ENTERPRISE

Remote installation of applications to computers of a client organization is identical to that within an enterprise (see the section "Remote installation of software" (see page 45)).

To install applications on computers of a client organization, the following conditions should be met:

- Before installing applications to client computers of the client enterprise for the first time, you should install Network Agent to 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 to 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 IP address or computer name in the Windows network.

- Select Using Microsoft Windows resources by means of Update Agents as 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 should have access to the Admin$ resource on all client computers.

CREATING A HIERARCHY OF ADMINISTRATION GROUPS SUBORDINATED TO THE VIRTUAL ADMINISTRATION SERVER

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

The procedure of creating a hierarchy of administration groups subordinate to virtual Administration Server is the same as procedure of creating a hierarchy of administration groups subordinate to 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 virtual Server's restriction described in Kaspersky Security Center Administrator's Guide.
REMOTE INSTALLATION OF APPLICATIONS

This section describes ways of installing and uninstalling Kaspersky Lab applications remotely.

Before you start installation of applications to client computers, make sure that the hardware and software on target computers meet the system requirements (see the section "Hardware and software requirements" on page 13).

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

Network Agent is a component that provides for Administration Server connection with client computers. This is why it must be installed on each client computer to be connected to the remote centralized control system.

The computer on which the Administration Server is 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. There is no need to install the Network Agent on that computer.

Network Agent can be installed remotely or locally like any application. During centralized deployment of anti-virus applications through Administration Console, you can install Network Agent jointly with anti-virus 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 computer once.

Kaspersky Lab applications are controlled through Administration Console by means of control plug-ins. Therefore, to access the application management interface through Kaspersky Security Center, the corresponding 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 computers only locally (for details refer to the manuals 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 completes with an error, you can find the cause of this error and fix it using the remote deployment preparation utility (see the section "Preparing computer for remote installation"). Utility tool riprep.exe" on page 54).

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

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

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4
- Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition
- Kaspersky Anti-Virus 8.0 for Storage
- Kaspersky Anti-Virus 5.7 for Novell NetWare®
- Kaspersky Anti-Virus 6.0 Second Opinion Solution
- Kaspersky Anti-Virus 8.0 for Linux File Server
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows
- Kaspersky Endpoint Security 8 for Smartphone
• Kaspersky Endpoint Security 8 for Mac
• Kaspersky Endpoint Security 8 for Linux
• Kaspersky Endpoint Security 10 for Mobile Devices
• Kaspersky Security for Virtualization 1.1
• Kaspersky Security for Virtualization 2.0.

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................................................................. 46
Installing applications using Remote Installation Wizard ............................................................... 49
Viewing a protection deployment report .......................................................................................... 49
Remote removal of applications ...................................................................................................... 50
Work with installation packages ..................................................................................................... 51
Retrieving up-to-date versions of applications ............................................................................... 53
Preparing computer for remote installation. Utility tool riprep.exe .................................................. 54

Installing Applications using a Remote Installation Task

You can deploy applications remotely on client computers by running remote installation tasks. Kaspersky Security Center allows you to create the following types of remote installation task:

• Group tasks. Tasks created for client computers of the selected administration groups.
• Tasks for specific computers. Tasks created for specific client computers depending on whether or not these computers belong to a particular administration group.

For correct remote installation on the client computer on which Network Agent has not been 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 client computers included in the domain. They open automatically using the Deployment preparation utility (see the section "Preparing computer for remote installation. Utility tool riprep.exe" on page 54).

In this section:

Installing an application on specific client computers ...................................................................... 46
Installing an application on client computers in the administration group ........................................ 47
Installing an application using Active Directory group policies ....................................................... 47
Installing applications on slave Administration Servers ..................................................................... 48

Installing an Application on Specific Client Computers

To install an application on specific client computers:

1. Establish a connection with the Administration Server that controls the relevant computers.
2. In the console tree, select the Tasks for specific computers folder.
3. Run the task creation by clicking the Create a task link.
   This starts the New Task Wizard. Follow the wizard's instructions.
   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 deployment of the selected application on specific computers. The new task appears in the workspace of the Tasks for specific computers 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 deployment task, the selected application will be installed on the specified client computers.

**INSTALLING AN APPLICATION ON CLIENT COMPUTERS IN THE ADMINISTRATION GROUP**

To install an application on client computers in the 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 wizard's instructions.
   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 deployment 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.
   On completion of the remote deployment task, the selected application will be installed on client computers 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 group remote installation task or remote installation task for specific computers.
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. After the task is started, the following objects are created in each domain that includes the client computers 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 computers 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 computers directly from the Kaspersky Security Center shared network folder KLSHARE. 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 computers 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, computers are added to the security group immediately.

4. When computers 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 the section "Distributing installation packages to slave Administration Servers" on page 52).

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

- If you want to create a task for the slave Servers of a selected administration group, run creation of a group task of remote installation for that group (see the section "Installing the application to client computers in an administration group" on page 47).
- If you want to create a task for selected slave Servers, run creation of a remote installation task for specific computers (see the section "Installing the application to selected client computers" on page 46).

This starts the New Task Wizard creating the remote deployment task. Follow the wizard's instructions.

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 to slave Administration Servers remotely.

The New Task Wizard will create the task of remote deployment 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 deployment 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 deployment of applications with specially created installation packages or directly from a distribution package.

For correct remote installation on the client computer on which Network Agent has not been installed, the following ports must be opened: TCP 139 and 445; UDP 137 and 138. By default, these ports are open for all computers included in the domain. They are opened automatically by using the Deployment preparation utility (see the section “Preparing computer for remote installation. Utility tool riprep” on page 54).

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 group workspace, open the Groups tab.
4. Launch application installation by clicking the Start installation link in the Remote installation section.

This will start the Remote Installation Wizard. Follow the wizard's instructions.

At the final step of the Wizard, click Next to create and launch the remote deployment task on the selected computers.

Kaspersky Security Center performs the following actions by using the Remote Installation Wizard:

- 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.
- Creates and starts a remote installation task for specific computers or for an administration group. The created remote deployment task is stored in the Tasks for specific computers folder or is 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: Installing <Installation package name>.

**VIEWING A PROTECTION DEPLOYMENT REPORT**

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

To view a protection deployment report:

1. Connect to an Administration Server from which a deployment report is required.
2. In the console tree, select the Reports and notifications folder.
3. In the Reports and notifications folder select the report template named Protection deployment report.

The results pane will display a report containing information about protection deployment on all client computers in the network.

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

- For an administration group
- For a set of client computers
- For a selection of client computers
- For all client computers

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 computer is covered by anti-virus protection if it has an anti-virus application installed and its real-time protection functionality is enabled.
REMOTE UNINSTALLATION OF APPLICATIONS

Kaspersky Security Center allows you to remove incompatible applications that may cause conflicts in the operation of Kaspersky Lab software managed via Kaspersky Security Center.

You can perform remote removal of applications from client computers by running remote removal tasks. Kaspersky Security Center allows you to create the following types of remote removal tasks:

- **Group tasks.** Tasks created for client computers of the selected administration groups.
- **Tasks for specific computers.** Tasks created for specific client computers depending on whether or not these computers belong to a particular administration group.

### IN THIS SECTION:

Remote removal of an application from client computers of the administration group ...............................................
Remote removal of an application from specific client computers .................................................................

## REMOTE REMOVAL OF AN APPLICATION FROM CLIENT COMPUTERS OF THE ADMINISTRATION GROUP

To remove an application remotely from client computers of the 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 wizard's instructions.

   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.

On completion of the remote removal task, the selected application will be removed from client computers in the administration group.

## REMOTE REMOVAL OF AN APPLICATION FROM SPECIFIC CLIENT COMPUTERS

To remove an application remotely from specific client computers:

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

   This starts the New Task Wizard. Follow the wizard's instructions.

   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 computers. The new task appears in the workspace of the **Tasks for specific computers** 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 removal task, the selected application will be removed from the specified client computers.
WORK WITH INSTALLATION PACKAGES

When creating remote installation tasks the system uses installation packages containing sets of parameters necessary for software installation. 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.................................................................................................................. 51
Distributing installation packages to slave Administration Servers................................................................. 52
Distributing installation packages by using Update Agents .............................................................................. 52
Transferring application installation results to Kaspersky Security Center ...................................................... 52

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 New → Installation package;
   • in the context menu of the list of installation packages, select New → Installation package;
   • click the Create installation package link in the installation package control section.

This will start the New Package Wizard. Follow the wizard's instructions.

When creating an installation package for the Kaspersky Lab application, you may be prompted to view the License Agreement for this application. Read the EULA 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 creating an installation package for an application from the Kaspersky Lab’s database of applications, you can enable automatic installation of system components (prerequisites) required for installation of the application. The Installation Package Creation Wizard displays a list of all available system components for the selected application. When creating a patch installation package (incomplete distribution package), a list contains all system prerequisites for 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 create the installation package for deployment of Network Agent manually. 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.

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 Servers, launch the creation of a task for specific computers.

   This starts the New Task Wizard. Follow the wizard's instructions.

   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 BY USING UPDATE AGENTS

You can use Update Agents to distribute installation packages within a group.

After the installation packages are received from the Administration Server, Update Agents automatically distribute them to client computers using multiaddress IP distribution. New installation packages are distributed within an administration group once. If a client computer has been disconnected from the corporate network at the time of distribution, Network Agent on the client computer automatically downloads the necessary installation package from an 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 URL 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.
PREPARING COMPUTER FOR REMOTE INSTALLATION.

UTILITY TOOL RIPREP.EXE

Application deployment to the client computer may complete with an error for the following reasons:

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

To solve problems that have occurred when installing the application on a client computer without the Network Agent installed, you can use the utility designed for preparation of computers to remote installation (riprep).

This section contains a description of the utility that allows you to prepare a computer for remote installation (riprep). The utility is located in the Kaspersky Security Center installation folder on the computer on which Administration Server is installed.

The utility used to prepare a computer for remote installation does not run under Microsoft Windows XP Home Edition.

In this section:

Preparing the computer for remote deployment in interactive mode ........................................ 54
Preparing the computer for remote deployment in non-interactive mode .................................. 55

PREPARING THE COMPUTER FOR REMOTE DEPLOYMENT IN INTERACTIVE MODE

To prepare the computer for remote deployment in the interactive mode:

1. Run the riprep.exe file on the client computer.
2. In the main window of the remote deployment 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 computer preparation for remote deployment are shown in the bottom 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 disabling of UAC, a prompt to restart the computer will be displayed.

**PREPARING THE COMPUTER FOR REMOTE DEPLOYMENT IN NON-INTERACTIVE MODE**

To prepare the computer for remote deployment in silent mode:

run the riprep.exe file on the client computer from the command line with the requisite 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 – Path to the configuration file (a file with the .ini extension).
- `-tl traceLevel` – Defines the trace level, where traceLevel – 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 simple file sharing;
- starting the Server service on the client computer;
- opening the ports;
- creating a local account;
- disabling User Account Control (UAC).

You can specify the settings for computer preparation for remote deployment in the configuration file specified in the `cfg` key. To specify 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 (UAC) (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 computer;
    - 1 – restart the computer, if UAC was enabled before starting the utility;
    - 2 – force restart, if UAC was enabled before starting the utility;
- 4—always restart the computer;
- 5—always restart the computer forcibly.

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 an installation procedure for applications that can be installed on a local computer only.

To perform local installation of applications on a specific client computer, you must have administrator rights on this computer.

To install applications locally on a specific client computer:

1. Install Network Agent on the client computer and configure the connection between the client computer and Administration Server.
2. Install the requisite applications on the computer as described in the manuals of these applications.
3. Install a control 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:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4
- Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition
- Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition
- Kaspersky Anti-Virus 8.0 for Storage
- Kaspersky Anti-Virus 6.0 Second Opinion Solution
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

LOCAL INSTALLATION OF NETWORK AGENT

To install the Network Agent to a computer locally:

1. Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center in the Packages\NetAgent folder.
   The Network Agent Installation Wizard starts. Follow the wizard’s instructions. 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.

2. If you want to use your computer as a connection gateway for a specific administration group, in the Connection gateway window of the Wizard, select Use as connection gateway.

3. If you install Network Agent to a virtual machine, you can perform the following actions:
   a. Enable dynamic mode of Network Agent for Virtual Desktop Infrastructure (VDI). To do this, in the Advanced Settings window of the Installation Wizard, select the Enable dynamic mode for VDI check box.
b. Optimize the operation of Network Agent. To do this, in the Advanced Settings window of the Installation 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 startup will be disabled. Also, sending of information about the following objects to Administration Server will be disabled:

- Hardware registry
- Applications installed on the local client computer
- Updates of Microsoft Windows that should be installed to the local client computer
- Software vulnerabilities detected on the local client computer.

You will be able to enable those features in the properties or policy settings of Network Agent.

After the Wizard completes, Network Agent will be installed on the computer.

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.

Network Agent is installed on the target computer together with a plug-in for work with Cisco® Network Admission Control (NAC). This plug-in is used if the computer has Cisco® Trust Agent installed.

## 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 to a local computer in non-interactive mode,
run the command

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

where `setup_parameters` is a list of settings and their respective values separated with commas

```bash
(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 16. Settings of Network Agent installation in non-interactive mode

<table>
<thead>
<tr>
<th>SETTING NAME</th>
<th>SETTING DESCRIPTION</th>
<th>AVAILABLE VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>Path to the Network Agent installation folder</td>
<td>String value</td>
</tr>
<tr>
<td>INSTALL_NSAC</td>
<td>Whether to install NAC</td>
<td>• 1 – Install</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other value or no value – Do not install</td>
</tr>
<tr>
<td>SERVERADDRESS</td>
<td>Administration Server address</td>
<td>String value</td>
</tr>
<tr>
<td>SERVERPORT</td>
<td>The port number to connect to the Administration Server</td>
<td>Numerical value</td>
</tr>
<tr>
<td>SERVERSSLPORT</td>
<td>Port number to connect to Administration Server by using SSL protocol</td>
<td>Numerical value</td>
</tr>
<tr>
<td>USESSL</td>
<td>Whether to use an SSL connection</td>
<td>• 1 – Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other value or no value – Do not use</td>
</tr>
<tr>
<td>OPENUDPPORT</td>
<td>Whether to open a UDP port</td>
<td>• 1 – Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other value or no value – Do not open</td>
</tr>
<tr>
<td>UDPPORT</td>
<td>UDP port number</td>
<td>Numerical value</td>
</tr>
</tbody>
</table>
### Local Installation of Applications

#### Management Plug-in

To install the application management plug-in:

On a computer that has Administration Console installed, run the executable file klcfginst.exe, 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.

### Setting Table

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Setting Description</th>
<th>Available Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>USEPROXY</td>
<td>Whether to use a proxy server</td>
<td>• 1 – Use&lt;br&gt;• Other value or no value – Do not use</td>
</tr>
<tr>
<td>PROXYADDRESS</td>
<td>Proxy address</td>
<td>String value</td>
</tr>
<tr>
<td>PROXYPORT</td>
<td>Number of a port for connection to Administration Server</td>
<td>Numerical value</td>
</tr>
<tr>
<td>PROXYLOGIN</td>
<td>Name of an account for connection to a proxy server</td>
<td>String value</td>
</tr>
<tr>
<td>PROXYPASSWORD</td>
<td>Password of an account for connection to a proxy server</td>
<td>String value</td>
</tr>
<tr>
<td>GATEWAYMODE</td>
<td>Connection gateway use mode:</td>
<td>• 0 – Do not use connection gateway&lt;br&gt;• 1 – Use the computer to which Network Agent is to be installed as connection gateway&lt;br&gt;• 2 – Connect to Administration Server via another connection gateway</td>
</tr>
<tr>
<td>GATEWAYADDRESS</td>
<td>Connection gateway address</td>
<td>String value</td>
</tr>
<tr>
<td>CERTSELECTION</td>
<td>Method of receiving a certificate</td>
<td>• GetOnFirstConnection – Receive an Administration Server certificate&lt;br&gt;• GetExistent – Select an existing certificate</td>
</tr>
<tr>
<td>CERTFILE</td>
<td>Path to the certificate file</td>
<td>String value</td>
</tr>
<tr>
<td>VMVDI</td>
<td>Whether to enable the dynamic mode for VDI</td>
<td>• 1 – Enable&lt;br&gt;• Other value or no value – Do not enable</td>
</tr>
<tr>
<td>LAUNCHPROGRAM</td>
<td>Whether to run the Network Agent service after installation completion</td>
<td>• 1 – Run&lt;br&gt;• Other value or no value – Do not run</td>
</tr>
</tbody>
</table>

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 website.
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 computer. Then open the folder just copied on the client computer.
   - From the client computer, open the shared folder on the Administration Server, which corresponds to the requisite installation package.
   - If the shared folder is located on a computer running under Microsoft Windows Vista, select the Disabled value for the User accounts management: all administrators operate in administrator approval mode setting (Start → Control Panel → Administrative Tools → 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 allows creating standalone installation packages for applications. A standalone installation package is an executable file that can be located on the web server, sent by email, or transferred to a client computer in any other way. The received file can be run locally on the client computer to install an application without involving Kaspersky Security Center.

To install an application using a standalone 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 in the workspace of the installation package.

This will start the Stand-alone Installation Package Creation Wizard. Follow the wizard's instructions.

At the final step of the Wizard, select a method of transferring the standalone installation package to the client computer.

5. Transfer the standalone installation package to the client computer.
6. Run the standalone installation package on the client computer.

As a result, the application is installed to the client computer with the settings specified in the standalone package.

When you create a standalone installation package, it is automatically published on Web Server. The link for downloading the standalone package is displayed on the list of created standalone installation packages. You can cancel publishing of the selected standalone package and republish it on the web server. By default, port 8060 is used for downloading standalone installation packages.
CONNECTION OF MOBILE DEVICES TO THE ADMINISTRATION SERVER

This section describes how to connect to Administration Server mobile devices supporting Exchange ActiveSync and iOS Mobile Device Management (iOS MDM) protocols.

IN THIS SECTION:

Mobile devices servers ................................................................. 61
Connecting mobile devices supporting Exchange ActiveSync ................................................................. 61
Connecting iOS MDM mobile devices ................................................................. 63

MOBILE DEVICES SERVERS

Mobile devices servers are designed to gather information about the user’s mobile devices and store their profiles. Mobile devices server is a component of Kaspersky Security Center that provides the administrator access to the user’s mobile devices and allows managing them through Administration Console.

There are two types of mobile devices servers:

- Mobile devices server supporting Exchange ActiveSync. Installed to a client computer where a Microsoft Exchange server has been installed, allowing retrieving data from the Microsoft Exchange server and passing them to Administration Server. This mobile devices server is used for management of mobile devices that support Exchange ActiveSync protocol.

- iOS MDM mobile devices server. It is installed to a client computer and allows connecting iOS mobile devices to Administration Server and managing iOS mobile devices via Apple Push Notifications (APNs) service.

After being installed to client computers, mobile devices servers are displayed in Administration Console, in the Mobile devices servers folder contained in the Mobile devices folder of the console tree.

Mobile devices servers of Kaspersky Security Center allow managing the following objects:

- Individual mobile devices and groups of mobile devices as a whole
- Several mobile devices connected to a cluster of servers, simultaneously. After connecting to a cluster of servers, the mobile devices server installed on this cluster is displayed in Administration Console as a single server.

CONNECTING MOBILE DEVICES SUPPORTING EXCHANGE ACTIVESYNC

Kaspersky Security Center allows managing Exchange ActiveSync mobile devices. Exchange ActiveSync mobile devices are mobile devices that are connected to mailboxes of a Microsoft Exchange server and managed over Exchange ActiveSync protocol.

The following operating systems support Exchange ActiveSync protocol:

- Windows Mobile
- Windows CE
- Windows Phone 7
- Windows Phone 8
- Android™
- Bada
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.

Connection of Exchange ActiveSync mobile devices to Administration Server is performed as follows:

1. The administrator installs Exchange ActiveSync Mobile Devices Server to a client computer with a Microsoft Exchange server installed on it. Installation of Exchange ActiveSync Mobile Devices Server is performed using standard tools of the operating system.
   After Exchange ActiveSync Mobile Devices Server is connected, it is displayed in Administration Console, in the Mobile devices servers subfolder contained in the Mobile devices folder of the console tree.
2. The administrator creates a management profile for Exchange ActiveSync mobile devices associated with a Microsoft Exchange mailbox.
   Management profile of Exchange ActiveSync mobile devices is an ActiveSync policy used on a Microsoft Exchange server for managing Exchange ActiveSync mobile devices.
3. The mobile device user connects to a Microsoft Exchange mailbox and receives a notification stating that the selected mailbox is managed by a profile, which imposes restrictions on the mobile device being connected.
   The user's mobile device connected to the Microsoft Exchange server is displayed in the Exchange ActiveSync mobile devices subfolder contained in the Mobile devices folder of the console tree.

After the Exchange ActiveSync mobile device is connected to Exchange ActiveSync 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.

In this section:

- Installing a Mobile devices server for Exchange ActiveSync ........................................... 62
- Creating a management profile for Exchange ActiveSync devices ...................................... 63

**Installing a Mobile devices server for Exchange ActiveSync**

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

To install an Exchange ActiveSync Mobile Devices Server to a local computer:

1. Copy the folder Packages\MDM4Exchange from Administration Server to a client computer.
2. Open the copied folder on the client computer and run the setup file setup.exe. The Exchange ActiveSync Mobile Devices Server Setup Wizard starts running.
3. Choose a type of Exchange ActiveSync Mobile devices server installation in Installation Setup window:
   - To install Exchange ActiveSync Mobile devices server with default settings, choose Standard Install and click Next.
   - To manually configure the Exchange ActiveSync Mobile devices server installation settings, choose Advanced Install 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 an installation mode for Exchange ActiveSync Mobile Devices Server 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 account. Account should be selected manually. Click Choose button, select the user account and specify password. The selected user should belong to a group with rights to manage mobile devices via ActiveSync.

d. In IIS Setup 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 "Windows authentication" mechanism manually in IIS settings for PowerShell Virtual Directory. If "Windows authentication" mechanism is disabled, Exchange ActiveSync Mobile devices server will not operate correctly. Please refer to IIS documentation for more information about configuring IIS.

e. Click Next.

4. Verify Exchange ActiveSync Mobile devices server installation properties in the next window, then click Install.

After the Wizard completes its operations, the Exchange ActiveSync Mobile Devices Server is installed to the local computer. The Exchange ActiveSync Mobile Devices Server will be displayed in the Mobile devices servers subfolder contained in the Mobile devices folder of the console tree.

**CREATING A MANAGEMENT PROFILE FOR EXCHANGE ACTIVESYNC DEVICES**

1. To create a management profile for Exchange ActiveSync mobile devices:
   1. In the Mobile devices folder of the console tree select the Mobile devices servers subfolder.
   2. In the workspace of the Mobile devices servers folder select an Exchange ActiveSync mobile devices server.
   3. Select Properties from the context menu of the Exchange ActiveSync Mobile devices server.

      The properties window of the Exchange ActiveSync Mobile devices server opens.

   4. In the properties window of the Exchange ActiveSync mobile devices server select the Mail boxes section.
   5. Select a mailbox and click the Change profiles button.

      The Settings profiles window opens.

   6. Click the Add button in the Settings profiles window.

      The New profile window opens.

   7. Configure the profile settings in the sections of the New profile window.
   8. Click OK.

      The profile will be displayed on the list of profiles in the Profiles window.

You can assign the "default profile" attribute to a management profile of Exchange ActiveSync mobile devices. Such profile is automatically assigned to new mailboxes and mailboxes with deleted profiles. The default profile cannot be deleted. To delete the current default profile, you should assign the "default profile" attribute to a different profile.

   To set the created profile as the default one,

      select the profile from the list in the Settings profiles window and click the Set as default profile button.

**CONNECTING iOS MDM MOBILE DEVICES**

Kaspersky Security Center allows managing mobile devices running under iOS. iOS MDM mobile devices are iOS mobile devices connected to an iOS MDM Mobile Devices Server and managed by Administration Server.
Connection of mobile devices to an iOS MDM Mobile Devices Server is performed as follows:

1. The administrator installs iOS MDM Mobile Devices Server to the selected client computer. Installation of iOS MDM Mobile Devices 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 the section "Receiving an APNs certificate" on page 65).
   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 to the iOS MDM Mobile Devices Server (see the section "Installing an APNs certificate to an iOS MDM Mobile Devices Server" on page 66).

4. The administrator creates an iOS MDM profile and sends a link for downloading the iOS MDM profile to the user of an iOS mobile device (see the section "Installing an iOS MDM profile to an iOS mobile device" on page 66).
   The iOS MDM profile contains a collection of settings for connection of iOS mobile devices to Administration Server. The mobile device user downloads and installs the profile to the device.

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

5. The administrator adds a configuration profile to the iOS MDM Mobile Devices Server (see the section "Adding a configuration profile to the iOS MDM Mobile Devices Server" on page 67 and installs the configuration profile to the mobile device after it is connected (see the section "Installing a configuration profile to an iOS MDM mobile device" on page 68).
   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 allows configuring iOS MDM mobile devices in accordance with the organization's security policies.

6. If necessary, the administrator adds provisioning profiles to the iOS MDM Mobile devices server (see the section "Adding a provisioning profile to an iOS MDM Mobile devices server" on page 68), and then installs the provisioning profiles to mobile devices (see the section "Installing a provisioning profile to an iOS MDM mobile device" on page 69).
   **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.

**INSTALLING IOS MDM MOBILE DEVICES SERVER**

To install an iOS MDM Mobile Devices Server to a local computer:

1. Copy the folder Packages\MDM4iOS from Administration Server to a client computer.

2. Open the copied folder on the client computer and run the setup file setup.exe.
   The iOS MDM Mobile Devices Server Installation Wizard starts running. Follow the instructions of the Setup Wizard.

3. 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.

4. In the **Settings for connection to iOS MDM mobile devices server** window of the Wizard, in the **External port to connect to iOS MDM service** field, specify an external port for connection of mobile devices to the iOS MDM service.
   The default port number is 443. Make sure that this port is not already in use for some other purpose.

5. If you want to configure interaction ports for application components manually, select the **Configure local ports manually** check box, and then specify values for the following settings:
   - **Network Agent connection port**. In this field specify a port for connection of the iOS MDM service to Network Agent. The default port number is 9799.
- **Port to connect to iOS MDM service.** In this field specify a local port for connection of Network Agent to the iOS MDM service. The default port number is 9899.

It is recommended to use default values.

6. In the **External server address** window of the Wizard, in the **URL address for remote connection with Mobile devices server** field, specify the address of a client computer to which the iOS MDM Mobile Devices Server will be installed.

This address will be used for connection of managed mobile devices to iOS MDM service. The client computer should be available for connection of iOS MDM mobile devices.

You can specify the address of a client computer in any of the following formats:
- FQDN name (such as mdm.example.com)
- NetBios name
- Computer IP address.

You do not have to add the URI scheme and the port number in the address string: those values will be added automatically.

When the Wizard finishes its operation, the iOS MDM Mobile devices server will be installed to the local computer. The iOS MDM Mobile devices server is displayed in the **Mobile devices servers** subfolder contained in the **Mobile devices** folder of the console tree.

**Receiving an APNs certificate**

Before receiving an APNs certificate, you should download Root Certificate and Application Integration certificate from Apple Inc. website [http://www.apple.com/certificateauthority/](http://www.apple.com/certificateauthority/), and then install them by using standard tools of your operating system. For details on how to download and install those certificates please refer to the Knowledge Base on the website of Kaspersky Lab Technical Support (article 9908).

When the Certificate Signing Request (CSR request) is created at the first step of APNs certificate wizard, its private key is stored in your computer'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 the **Mobile devices servers** subfolder.
2. In the workspace of the **Mobile devices servers** folder select an iOS MDM mobile devices server.
3. Select **Properties** from the context menu of the iOS MDM mobile devices server.

The properties window of the iOS MDM mobile devices server opens.

4. In the properties window of the iOS MDM Mobile devices server select the **Certificates** section.
5. In the **Certificates** section, in the **Apple Push Notification certificate** group of settings, click the **Request new** button.

APNs certificate wizard will be launched with **Request New APNs Certificate** window open.

6. 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 will be saved in the computer memory.

7. Send the file with your CSR request to Kaspersky Lab for signing via your CompanyAccount (see the section “Obtaining technical support via Kaspersky CompanyAccount” on page 77).

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

After your online request is processed, you will receive a CSR request file signed by Kaspersky Lab.
8. 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.

9. 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 ОК.  
      This password will be used to install the APNs certificate on iOS MDM Mobile Devices 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 to the iOS MDM Mobile Devices Server (see section "Installing an APNs certificate to an iOS MDM Mobile Devices Server" on page 66).

For more detailed instructions on how to create a CSR request and send it to Apple Inc., please refer to the Knowledge Base on the Kaspersky Lab Technical Support website (article 9245).

**INSTALLING AN APNs CERTIFICATE TO AN iOS MDM MOBILE DEVICES SERVER**

After you have received the APNs certificate, you should install it to the iOS MDM Mobile devices server.

**To install an APNs certificate to an iOS MDM Mobile Devices Server:**

1. In the Mobile devices folder of the console tree select the Mobile devices servers subfolder.
2. In the workspace of the Mobile devices servers folder select an iOS MDM mobile devices server.
3. Select Properties from the context menu of the iOS MDM Mobile devices server.
   The properties window of the iOS MDM mobile devices server opens.
4. In the properties window of the iOS MDM Mobile devices server select the Certificates section.
5. In the Certificates section, in the Apple Push Notification certificate group of settings click the Install button.
6. Select the PFX file that contains the APNs certificate.
7. Enter the password of the private key specified when exporting the APNs certificate (see the section "Receiving an APNs certificate" on page 65).

As a result, the APNs certificate will be installed to the iOS MDM Mobile devices server. Certificate details will be displayed in the properties window of the iOS MDM Mobile devices server, in the Certificates section.

**INSTALLING AN iOS MDM PROFILE TO IOS MOBILE DEVICE**

To manage users’ mobile devices with the iOS MDM Mobile devices server, you should create an iOS MDM profile and install it to mobile devices.

**To create an iOS MDM profile and install it to a mobile device:**

1. In the console tree select the User accounts folder.
2. Select an account of user on whose mobile device you want to install an iOS MDM profile.
3. In the context menu of the mobile user device account select **Install iOS MDM profile to user mobile device**. The **iOS MDM profile installation** window opens.

4. In the **iOS MDM profile installation** window, in the **List of available iOS MDM mobile devices servers** field select iOS MDM mobile devices server for which you need to create an iOS MDM profile.

5. If you want to use a certificate other than the one generated by Administration Server to set for the iOS MDM profile, select the **Specify another certificate** check box and define the certificate settings.

6. In the **iOS MDM profile installation** window, specify a method of sending to the user a notification with a link for downloading the iOS MDM profile:
   - If you want to send the user a notification in an SMS message, select the **By SMS** check box. In the **SMS text** field enter a message for the user or use the default message.
     
     Delivery of notifications by SMS is available if the following requirements are met: A GSM module is integrated in users' devices, SMS delivery via Kaspersky SMS Broadcasting utility is set up in Kaspersky Security Center (see the section "Configuring SMS delivery in Kaspersky Security Center" on page [70](#)), and users' phone numbers are specified in their accounts.

   - If you want to send the user a notification and an exclusively created QR code by email, select the **Email** check box. In the **Subject** field enter the message subject. In the **Notification message** field, enter a message for the user or use the default message.
     
     If you have changed the standard text of the SMS message or the email notification, check the **SMS text** or **Notification message** field for the variable `%URL%`. The variable `%URL%` contains a link for the user to download the iOS MDM profile to the device. It is recommended to avoid changing its name.

     You can add the variable `%URL%` to a message text by clicking the arrow button and selecting **One-time link** from the menu that opens.

7. Click **OK**.

As a result, the iOS MDM profile is automatically published on the web server. The mobile device user receives the notification with the link for downloading the iOS MDM profile. The user clicks the link. After that, the device's operating system prompts the user to accept the installation of the iOS MDM profile. If the user accepts the profile installation, the iOS MDM profile will be downloaded to the device. After the profile is successfully installed to the user's mobile device, it is automatically deleted from the web server. By default, port 8061 is used for downloading the iOS MDM profile.

To allow the user to proceed to Kaspersky Security Center web portal, a connection with Administration Server via port 8061 should be available on the mobile device.

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

### Adding a Configuration Profile to an iOS MDM Mobile Devices Server

To create a configuration profile, you should install iPhone Configuration Utility to the computer where Administration Console is installed. You should download iPhone Configuration Utility from Apple Inc. website and install it by using standard tools of your operating system.

1. In the **Mobile devices** folder of the console tree select the **Mobile devices servers** subfolder.
2. In the workspace of the **Mobile devices servers** folder select an iOS MDM mobile devices server.
3. Select **Properties** from the context menu of the iOS MDM Mobile devices server.
   
   The Mobile devices server properties window opens.
4. In the properties window of the **Mobile devices server** select the **Profiles** section.
5. Click the Create button in the Profiles section.
The Add new configuration profile window opens.

6. In the Add new configuration profile window, specify a profile name in the Configuration profile name field.

7. In the Add configuration profile window, in the Configuration profile ID field, specify the ID of the configuration profile to be created. The configuration profile ID should be unique; the value should be specified in Reverse-DNS format, for example, com.companyname.identifier.

8. Click OK.
   An application named iPhone Configuration Utility then starts.

9. Reconfigure the profile in iPhone Configuration Utility.
   For a description of the profile settings and instructions on how to configure the profile, please refer to the documentation enclosed with iPhone Configuration Utility.

After you have configured the profile with iPhone Configuration Utility, the new configuration profile is displayed in the Profiles section in the properties window of the iOS MDM Mobile devices server.

The created profile should be installed to iOS MDM mobile devices (see the section “Installing a configuration profile to an iOS MDM mobile device” on page 68).

**INSTALLING A CONFIGURATION PROFILE TO AN iOS MDM MOBILE DEVICE**

- To install a configuration profile to an iOS MDM mobile device:
  1. In the Mobile devices folder of the console tree select the iOS MDM mobile devices subfolder.
  2. In the iOS MDM mobile devices folder select a mobile device to which you want to install a configuration profile.
  3. In the mobile device context menu select the Install profile to device or use the corresponding option from the Actions menu.
     The Select profile to be installed window opens.
  4. In the Select profile to be installed window select a configuration profile.
  5. Click OK.
     The configuration profile will be installed to the iOS MDM mobile device.

**ADDING A PROVISIONING PROFILE TO AN iOS MDM MOBILE DEVICES SERVER**

Before adding a provisioning profile to the iOS MDM Mobile devices server, you should create one on Apple Developer Portal https://developer.apple.com/.

- To add a provisioning profile to iOS MDM mobile devices server:
  1. In the Managing mobile devices folder of the console tree select the Mobile devices servers subfolder.
  2. In the workspace of the Mobile devices servers folder select an iOS MDM mobile devices server.
  3. Select Properties from the context menu of the iOS MDM Mobile devices server.
     The Mobile devices server properties window opens.
  4. In the Mobile devices servers properties window, click the Import button and specify the path to a provisioning profile file.
     The profile will be added to the iOS MDM mobile devices server settings.
Installing a Provisioning Profile to an iOS Mobile Device

To install a provisioning profile to an iOS MDM mobile device:

1. In the Mobile devices folder of the console tree select the iOS MDM mobile devices subfolder.
2. In the workspace of the iOS MDM mobile devices folder select mobile device to which you want to install a provisioning profile.
3. In the device context menu, select the Install provisioning profile to device or select the corresponding option in the Actions menu.
   - The Select provisioning profile to be installed window opens.
4. In the Select provisioning profile to be installed window specify the provisioning profile that you want to install to mobile device.
5. Click OK.
   - Provisioning profile will be installed to the mobile device.
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 computers
- 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 ................................................................. 70
Synchronization of a mobile device with Administration Server ........................................................................ 71
Assigning a mobile device as the SMS sender .............................................................................................. 71

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.

2. In the workspace of the Installation packages folder click the Manage packages of mobile applications link to open the Mobile applications packages management window.

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 application 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 application package containing Kaspersky SMS Broadcasting utility.
6. Download the mobile application package containing 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 Kaspersky SMS Broadcasting utility to your mobile device from the Kaspersky Lab website, or connect your mobile device to a computer and copy to the mobile device 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, from the context menu of the Reports and notifications folder select Properties. The Properties dialog will appear. Reports and notifications folder.
  2. In the Properties: Reports and notifications window, select the SMS senders section.
  3. Click the Add button in the SMS senders section.
  4. In the Select device window specify a mobile device that will be used as the SMS sender.
  5. Click OK.

Kaspersky SMS Broadcasting utility should be installed on the device assigned as the SMS sender.
NETWORK LOAD

This section contains information about the volume of network traffic that the client computers and the Administration Server exchange during key administrative scenarios.

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
- Checking of connection between a client computer and Administration Server
- Regular update of anti-virus databases
- processing of events on client computers by the Administration Server.

IN THIS SECTION:

Table 17. Traffic per 24 hours

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Network Agent installation for a single client computer</th>
<th>Installing Kaspersky Endpoint Security 10 for Windows to one client computer (with databases updated)</th>
<th>Concurrent installation of the Network Agent and Kaspersky Endpoint Security 10 for Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic from client computer to Administration Server, KB</td>
<td>386.70</td>
<td>1,841.3</td>
<td>2,253.8</td>
</tr>
<tr>
<td>Traffic from Administration Server to client computer, KB</td>
<td>14,801.13</td>
<td>269,994.5</td>
<td>284,768.7</td>
</tr>
<tr>
<td>Total traffic (for a single client computer), KB</td>
<td>15,187.83</td>
<td>271,835.8</td>
<td>287,022.5</td>
</tr>
</tbody>
</table>
After the Network Agents are installed on the target client computers, one of the computers in the administration group can be assigned to function as an Update Agent. It will be used for distribution of installation packages. In this case, traffic volume transferred during initial deployment of anti-virus protection varies considerably depending on whether the multicast IP delivery is used or not.

If the multicast IP delivery is used, installation packages will be once sent to all running computers in the administration group. Thus, total traffic will become N times smaller, where N stands for the total number of running computers in the administration group. If the multicast IP delivery is not used, the total traffic is identical to the traffic when the distribution packages are downloaded from the Administration Server. However, the package source will be the Update Agent, not the Administration Server.

**INITIAL UPDATE OF THE ANTI-VIRUS DATABASES**

This section provides information about traffic volume values when starting the database update task for the first time (see table below).

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Initial Update of the Anti-virus Databases¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic from client computer to Administration Server, KB</td>
<td>1,357.1</td>
</tr>
<tr>
<td>Traffic from Administration Server to client computer, KB</td>
<td>33,917.0</td>
</tr>
<tr>
<td>Total traffic (for a single client computer), KB</td>
<td>35,274.1</td>
</tr>
</tbody>
</table>

**SYNCHRONIZING A CLIENT WITH THE ADMINISTRATION SERVER**

This scenario describes the state of the administration system when intensive data synchronization occurs between a client computer and the Administration Server. Client computers connect to the Administration Server with the administrator-defined interval. The Administration Server compares the status of data on a client computer with that on the Server, records information about the last client computer connection in 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).

¹ The data in the table may vary slightly depending upon the current anti-virus database version.
Table 19. Traffic

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Traffic from client computers to Administration Server, KB</th>
<th>Traffic from Administration Server to client computers, KB</th>
<th>Total traffic (for a single client computer), KB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INITIAL SYNCHRONIZATION</strong>3 PRIOR TO UPDATING DATABASES ON A CLIENT COMPUTER</td>
<td>368.6</td>
<td>463.7</td>
<td>832.3</td>
</tr>
<tr>
<td><strong>INITIAL SYNCHRONIZATION</strong>4 AFTER UPDATING DATABASES ON A CLIENT COMPUTER</td>
<td>1,748.3</td>
<td>34,388.3</td>
<td>36,136.6</td>
</tr>
<tr>
<td><strong>SYNCHRONIZATION WITH NO CHANGES ON A CLIENT COMPUTER AND THE ADMINISTRATION SERVER</strong></td>
<td>8.7</td>
<td>6.6</td>
<td>15.3</td>
</tr>
<tr>
<td><strong>SYNCHRONIZATION AFTER CHANGING THE VALUE OF A SETTING IN A GROUP POLICY</strong>5</td>
<td>11.1</td>
<td>13.3</td>
<td>24.4</td>
</tr>
<tr>
<td><strong>SYNCHRONIZATION AFTER CHANGING THE VALUE OF A SETTING IN A GROUP TASK</strong></td>
<td>10.0</td>
<td>12.5</td>
<td>22.5</td>
</tr>
<tr>
<td><strong>FORCED SYNCHRONIZATION WITH NO CHANGES ON A CLIENT COMPUTER</strong></td>
<td>47.3</td>
<td>15.5</td>
<td>62.8</td>
</tr>
</tbody>
</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).

Table 20. Traffic

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Incremental update of anti-virus databases6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic from client computer to Administration Server, KB</td>
<td>436.9</td>
</tr>
<tr>
<td>Traffic from Administration Server to client computer, KB</td>
<td>9,979.2</td>
</tr>
<tr>
<td>Total traffic (for a single client computer), KB7</td>
<td>10,416.1</td>
</tr>
</tbody>
</table>

3 Traffic volume varies considerably depending on whether the multicast IP delivery is used within administration groups or not. If the multiaddress IP delivery option is used, the total traffic volume decreases approximately by \( N \) times for the group, where \( N \) stands for the total number of computers included in the administration group.

4 Installing Network Agent and the anti-virus application to the client computer, moving the client computer to an administration group, applying a policy and default group tasks to the client computer.

5 Installing Network Agent and the anti-virus application to the client computer, moving the client computer to an administration group, applying a policy and default group tasks to the client computer.

6 The table specifies traffic rates in case of modifying a password-protected setting comprised in the Kaspersky Endpoint Security policy settings. Data for other policy settings may differ from those displayed in the table.

7 Traffic volume may vary considerably depending on whether the multicast IP delivery is used within administration groups or not. If the multiaddress IP delivery option is used, the total traffic volume decreases approximately by \( N \) times for the group, where \( N \) stands for the total number of computers included in the administration group.
PROCESSING OF EVENTS FROM CLIENTS BY ADMINISTRATION SERVER

This section provides information about traffic volume values when a client computer encounters a "Virus detected" event, which is then sent to the Administration Server and registered in the database (see the table below).

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Data transfer to Administration Server upon a &quot;Virus detected&quot; event</th>
<th>Data transfer to Administration Server upon nine &quot;Virus detected&quot; events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic from client computer to Administration Server, KB</td>
<td>27.2</td>
<td>100.4</td>
</tr>
<tr>
<td>Traffic from Administration Server to client computer, KB</td>
<td>25.8</td>
<td>52.5</td>
</tr>
<tr>
<td>Total traffic (for a single client computer), KB</td>
<td>53.0</td>
<td>152.9</td>
</tr>
</tbody>
</table>

**Traffic per 24 hours**

This section contains information about traffic rates for 24 hours of the administration system's activity in "quiet" condition, when no data changes are made both by client computers and by the Administration Server (see table below).

<table>
<thead>
<tr>
<th>Scenario</th>
<th>&quot;Idle&quot; state of the administration system⁹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic from client computer to Administration Server, KB</td>
<td>2,922.1</td>
</tr>
<tr>
<td>Traffic from Administration Server to client computer, KB</td>
<td>15,140.5</td>
</tr>
<tr>
<td>Total traffic (for a single client computer), KB</td>
<td>18,062.6</td>
</tr>
</tbody>
</table>

⁹ Data in the table can 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.

⁹ 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 frequency of synchronization of the client computer with Administration Server was 20 minutes, updates were downloaded to the Administration Server storage once per hour.
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.

(\(N_e^*N_h\)) events per day are added to the database (see table below). Here \(N_h\) is the number of client devices where managed applications are installed, \(N_e\) is the number of events per day that are informed of by a managed application installed on a client device.

<table>
<thead>
<tr>
<th>Number of Devices Where Managed Applications Are Installed</th>
<th>Number of Events Added to the Database Per Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>(\leq 2,000)</td>
</tr>
<tr>
<td>1000</td>
<td>(\leq 20,000)</td>
</tr>
<tr>
<td>10,000</td>
<td>(\leq 200,000)</td>
</tr>
</tbody>
</table>

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 Settings section of the properties window of Administration Server. By default, the database contains not more than 400,000 events.
CONTACTING TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and what conditions should be met to receive help from the Technical Support Service.

IN THIS SECTION:

How to obtain technical support................................................................. 77
Technical support by phone ........................................................................... 77
Obtaining technical support via Kaspersky CompanyAccount............................. 77

HOW TO OBTAIN TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (see the section "Sources of information about the application" on page 9), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support specialists will answer your questions about installing and using the application.

Before contacting Technical Support, we recommend that you read through the support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a request via Kaspersky CompanyAccount on Technical Support website. This method allows you to contact Technical Support specialists through a request form.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support (http://support.kaspersky.com/b2b) by phone.

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules). This will allow our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount is a web service (https://companyaccount.kaspersky.com) designed for sending and tracking requests to Kaspersky Lab.

To access Kaspersky CompanyAccount, register on the registration page (https://support.kaspersky.com/companyaccount/registration) and obtain a login and password. To do this, you should specify your activation code or key file.

In Kaspersky CompanyAccount you can perform the following actions:

- contact the Technical Support Service and Virus Lab;
- contact the Technical Support Service without using email;
- Track the status of your requests in real time.
• view a detailed history of your requests to the Technical Support Service;
• receive a copy of the key file if it has been lost or removed.

Technical Support by email

You can send an online request to Technical Support in English, Russian, and other languages.

You should specify the following data in the fields of the online request form:
• request type;
• application name and version number;
• request description.

If necessary, you can also attach files to the online request form.

A specialist from Technical Support Service sends an answer to your question via Kaspersky CompanyAccount to the email address that you have specified during your registration.

Online request to the Virus Lab

Some requests should be sent to the Virus Lab instead of the Technical Support Service.

You can send requests to the Virus Lab in the following cases:
• If you suspect that a file or a web resource contains a virus, but Kaspersky Security Center does not detect any threats. Virus Lab specialists analyze the file or web resource sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating Kaspersky Lab anti-virus applications.
• If Kaspersky Security Center classifies a file or a web resource as containing a virus, but you are sure that it poses no threat.

You can also send requests to the Virus Lab from the request form page (http://support.kaspersky.com/virlab/helpdesk.html) without having a registered Kaspersky CompanyAccount. You do not have to specify the application activation code. The priorities of requests generated in the request form are lower than those of requests generated via Kaspersky CompanyAccount.
GLOSSARY

**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 Server**
A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

**Administration Server Certificate**
The certificate used for the Administration Server authentication during connection of Administration Consoles to it and data exchange with client computers. 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 Computer)**
A computer, server, or workstation on which Network Agent and managed Kaspersky Lab applications are running.

**Administration Server Data Backup**
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 information about the structure of administration groups and client computers
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate.

**Administration Group**
A set of computers grouped together in accordance with the performed functions and the Kaspersky Lab applications installed on those machines. Computers are grouped for convenience of management as one single entity. A group can include other groups. A group can contain group policies for each application installed in it and appropriate group tasks.

**Administrator’s Workstation**
Computer 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.

**Application Management Plug-in**
A specialized component that provides the interface for application management through Administration Console. Each application has its own plug-in. It is included in all Kaspersky Lab applications that can be managed by using Kaspersky Security Center.
**APPLICATION SETTINGS**

Operational settings of the application that are common for all task types, defining the whole application operation, for example: application performance settings, reports settings, 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.

**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**

**DATABASES**

Databases that contain information about computer security threats that are known to Kaspersky Lab at the time of release of the databases. Records that are contained in databases allow detecting malicious code in scanned objects. The databases are created by Kaspersky Lab specialists and updated hourly.

**DIRECT APPLICATION MANAGEMENT**

Application management through a local interface.

**E**

**EVENT SEVERITY**

Property of an event encountered during the operation of a Kaspersky Lab application. There are four severity levels:

- Critical event.
- Error.
- Warning.
- Info.

Events of the same type can have different severity levels depending on the situation in which the event occurred.

**EXCHANGE ACTIVESYNC MOBILE DEVICE**

Mobile device connected to Administration Server over Exchange ActiveSync protocol.

**EXCHANGE ACTIVESYNC MOBILE DEVICE SERVER**

A component of Kaspersky Security Center that is installed in a client computer, allowing Exchange ActiveSync mobile devices to connect to Administration Server.
**G**

**GROUP TASK**
A task defined for an administration group and performed on all client computers within this 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. An installation package is created based on special files with the .kpd and .kud extensions that are included in the application distribution package; it contains a set of settings required for application setup and its configuration for normal functioning immediately after installation. Parameter values correspond to application defaults.

**iOS MDM MOBILE DEVICE**
Mobile device under iOS platform managed by the iOS MDM Mobile Devices Server (see the section “iOS MDM Mobile Devices Server” on page 81).

**iOS MDM MOBILE DEVICES SERVER**
A component of Kaspersky Security Center, installed to a client computer and allowing connection of iOS mobile devices to Administration Server and management of iOS mobile devices through Apple Push Notifications (APNs) service.

**iOS MDM PROFILE**
Collection of settings for connection of 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.

**K**

**KASPERSKY LAB UPDATE SERVERS**
HTTP and FTP servers at Kaspersky Lab from which Kaspersky Lab applications retrieve updates for databases and application modules.

**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 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 OPERATOR**
A component of Kaspersky Security Center installed together with Administration Server. Web Server is designed for transfer of standalone installation packages, iOS MDM profiles, and files from the shared folder over the network.

**KEY FILE**
A file in xxxxxxx.xkey 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.
LICENSE VALIDITY PERIOD
License term is a 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 computer.

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 logs in to the domain, the system attempts to install the application on the corresponding client computer. This method is recommended for remote installation of the company's applications to computers running Microsoft Windows 98 / Me operating systems.

MOBILE DEVICES SERVER
A component of Kaspersky Security Center that provides access to mobile devices and allows managing them through Administration Console.

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.

POLICY
A set of application settings in an administration group managed through Kaspersky Security Center. Application settings can differ in various groups. A specific policy is defined for each application. A policy includes the settings for complete configuration of all application features.

PROFILE
A 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 computer 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.

PUSH INSTALLATION
Method for remote installation of Kaspersky Lab applications, which lets you install software on the specified client hosts. For successful push install completion, the account used for the task must have sufficient rights to start applications remotely on client computers. This method is recommended for installing software on computers running Microsoft Windows NT / 2000 / 2003 / XP operating systems and supporting that functionality or to computers running Microsoft Windows 98 / Me with the Network Agent installed.
**R**

**REMOTE INSTALL**
Installation of Kaspersky Lab applications by using the services 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 information about the structure of administration groups and client computers
- 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 a Kaspersky Lab application are implemented as tasks, for example: Real-time protection, Full Scan, Databases update.

**TASK FOR SPECIFIC COMPUTERS**
A task assigned for a set of client computers from arbitrary administration groups and performed on those hosts.

**TASK SETTINGS**
Task-specific application settings.

**U**

**UPDATE**
The procedure of replacing / adding new files (databases or application modules) received from Kaspersky Lab update servers.

**UPDATE AGENT**
Computer acting as an intermediate source for distribution of updates and installation packages in an administration group.

**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.
KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

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). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey “TGI-Russia 2009”.

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company’s activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab’s products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab’s centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab’s products are certified by the 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’s virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. Kaspersky Lab’s Anti-Virus database is updated hourly; and the Anti-Spam database every five minutes.

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 many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), Communigate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), Watchguard Technologies (USA), and ZyXEL Communications (Taiwan). 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 2010 Kaspersky Anti-Virus received a few top Advanced+ awards in a test held by AV-Comparatives, an acknowledged Austrian anti-virus laboratory. But Kaspersky Lab’s main achievement is the loyalty of its users worldwide. The company’s products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab’s website: http://www.kaspersky.com
Virus encyclopedia: http://www.securelist.com
Anti-Virus Lab: newvirus@kaspersky.com (only for sending probably infected files in archives)
http://support.kaspersky.com/virlab/helpdesk.html (for queries addressed to virus analysts)
Kaspersky Lab’s web forum: http://forum.kaspersky.com
ABOUT NAC/ARP ENFORCEMENT TECHNOLOGY

The NAC Solution/ARP Enforcement technology is legal technology dedicated to securing and regulating access to a corporate network by ensuring device compliance to corporate security policies.

User behavior and user obligations

The user agrees to comply with the applicable local, state, national, international, and supranational laws and regulations as well as the specifications mentioned in the documentation or the related transfer documents of the authorized dealer from whom the user purchased the Software and

- (a) not to use the Software for illegal purposes,
- (b) not to transmit or store material that infringes intellectual property rights or any other rights of third parties or is illegal, unauthorized, defamatory or offensive or invades the privacy of third parties,
- (c) not to transmit or store data owned by third parties, without obtaining beforehand the consent prescribed by law of the owner of the data to the data transmission,
- (d) not to transmit material containing software viruses or any other harmful computer codes, files or programs,
- (e) not to carry out any acts interfering with or interrupting the operation of the server or networks associated with the software,
- (f) not to attempt to gain unauthorized access to computer systems or networks associated with the Software.

The user is restricted to using the software as intended and within the specific legal framework conditions in their country. Please note that the use of this security Software within networks can affect provisions of data protection law at the EU level and/or at EU member state level. Moreover, in operational use also provisions of collective labor law may have to be observed.
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 NOTICE

Registered trademarks and service marks are the property of their owners.
Active Directory, Data Access, Internet Explorer, Microsoft, SQL Server, Windows, Windows Server and Windows Vista are trademarks of Microsoft Corporation registered in the United States and elsewhere.
Android is a trademark owned by Google, Inc.
Apache and the Apache feather logo are trademarks owned by the Apache Software Foundation.
Apple, iPhone, Mac and Mac OS are registered trademarks of Apple Inc.
Cisco is a registered trademark or trademark of Cisco Systems, Inc. and / or its affiliates in the United States and certain other countries.
Intel, Core and Xeon are trademarks of Intel Corporation in the U.S. and / or other countries.
Linux is a trademark owned by Linus Torvalds and registered in the U.S. and elsewhere.
Novell, Netware are trademarks of Novell Inc. registered in the United States and elsewhere.
UNIX is a trademark registered in the U.S. and elsewhere; use under license from X/Open Company Limited.
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 ........................................................................................................... 47
Adding
   Administration Server ......................................................................................... 40, 44
Administration Console .............................................................................................. 29
Administration groups ................................................................................................. 44
Administration Server ................................................................................................. 29, 32
B
Building defense ............................................................................................................ 19
C
Cisco Network Admission Control ............................................................................ 29
Connection gateway .................................................................................................... 19, 43, 57
Custom installation ..................................................................................................... 28
D
Database ...................................................................................................................... 13, 30
Deployment preparation utility .................................................................................... 45, 49, 54
Deployment schemes .................................................................................................. 19
Distribution of installation package ............................................................................ 52
E
eexec ............................................................................................................................ 47
F
File with application description ................................................................................ 52
H
Hardware requirements ............................................................................................... 13
I
Installation
   Active Directory .................................................................................................... 45, 47
   Custom .................................................................................................................. 28
   Kaspersky Security Center .................................................................................... 25
   Local ...................................................................................................................... 57
   Logon script .......................................................................................................... 46
   Non-interactive mode ............................................................................................ 59
   Push ....................................................................................................................... 46
   Remote .................................................................................................................. 45
   Selecting components ........................................................................................... 29
   Slave Administration Server ............................................................................... 48
   Standalone package ............................................................................................... 45, 60
   Task ...................................................................................................................... 45
Installation package
   distribution .............................................................................................................. 44, 51
   distribution ............................................................................................................ 52
K
Kaspersky Lab SHV ...................................................................................................... 29
Kaspersky Lab ZAO ..................................................................................................... 84
kbackup ....................................................................................................................... 25
klrsrvswch .................................................................................................................. 30
kpd-file.............................................................. 52

L
Local System Account ........................................ 30
Logon script.................................................... 46

M
Mobile devices................................................... 32
Mobile devices support ........................................ 29

N
Network Agent .................................................. 29, 32
  Installation ................................................... 43, 57
Network discovery ............................................. 42
Network Size ................................................... 29

P
Packages ........................................................ 51
Ports ............................................................. 26
Posture Validation Server ................................... 29, 32
Push installation ............................................... 46

R
Remote Installation Wizard .................................. 49
Remove
  Kaspersky Security Center .................................. 37
    Task ....................................................... 50
Reports ........................................................ 49
triprep .......................................................... 54

S
Service
  Administration Server ..................................... 32
  Network Agent .............................................. 32
  Posture Validation Server ................................ 32
Settings
  kpd-file .................................................... 52
Shared folder .................................................. 31
Slave Servers
  Adding ...................................................... 44
SNMP agent .................................................... 29
Software requirements ...................................... 13
SQL-server .................................................... 30
Standalone installation package ......................... 45, 60
Stress testing ................................................ 19

T
Task .................................................................. 46
Typical installation ........................................... 27

U
Update Agents .................................................. 42, 43, 44, 52
Updating the application ..................................... 25
User account ................................................... 30