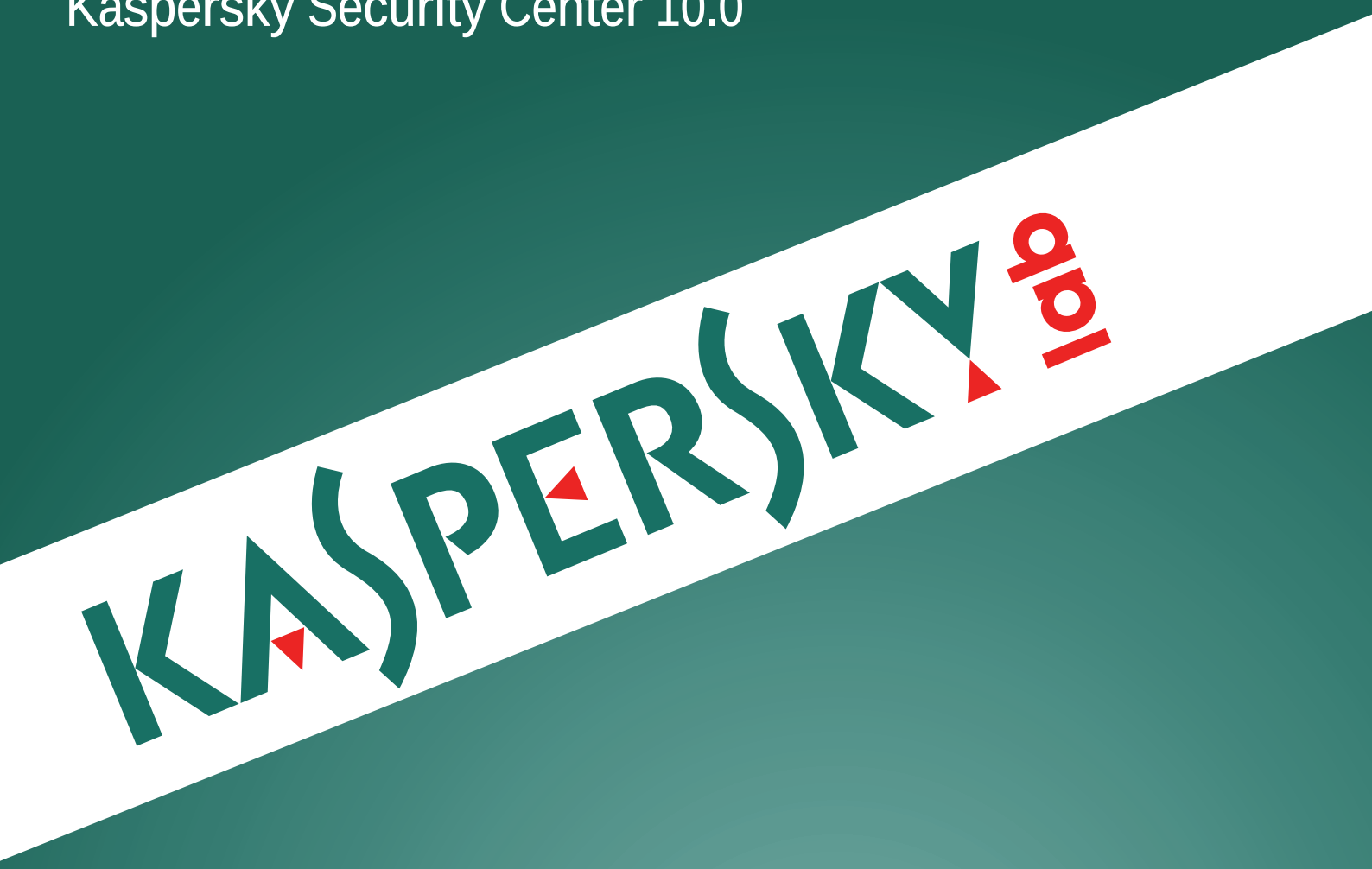
Kaspersky Security Center 10.0



Implementation Guide

APPLICATION VERSION: 10.0

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

This document may be amended without prior notice. 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: 12/17/2012

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

CONTENT

ABOUT THIS GUIDE

This document is the Implementation Guide for Kaspersky Security Center 10.0 (hereinafter also 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 do the following:

- Provide a general description of Kaspersky Security Center operating principles, system requirements, standard deployment scenarios, and particularities of integration with other applications.
- Help to plan the deployment of Kaspersky Security Center in the local area 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

The Kaspersky Security Center Implementation Guide contains an introduction, sections describing application components and their interaction configuration, sections describing how to deploy anti-virus protection on a network, sections containing stress testing results, and an index.

Sources of information about the application (see page 10)

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 12)

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

Application architecture (see page 13)

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

Hardware and software requirements (see page 14)

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

Information about Administration Server performance (see page 17)

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

Typical schemes of protection system deployment (see page 20)

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

Deploying a protection system within an organization (see page 21)

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

Deploying a protection system on a client organization's network (see page 24)

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 27)

This section describes stages of Administration Server deployment.

Configuring a protection system for a client organization's network (see page 44)

This section describes the features of setup of a protection system using Administration Console on a client enterprise network.

Remote deployment of applications (see page 48)

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

Local installation of applications (see page 62)

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

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.

Configuring SMS delivery in Kaspersky Security Center (on page 72)

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

Network load (see page 75)

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 79)

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

This section explains how to contact Technical Support Service.

Glossary

This section lists terms used in the guide.

Kaspersky Lab ZAO (see page 87)

This section provides information about Kaspersky Lab ZAO.

Information on the third-party code (see page 88)

This section provides information about third-party code used in Kaspersky Security Center.

Trademark notice (see page 89)

This section contains registered trademark notices.

Index

Using this section, you can easily find the required data in the document.

DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

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

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
We recommend that you use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.
Example: ...	Examples are given on a yellow background under the heading "Example".

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • New terms • Names of application statuses and events.
Press **ENTER**. Press **ALT**+**F4**.	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the **Enable** button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ *To configure a task schedule:*	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
Enter `help` in the command line The following message then appears: `Specify the date in dd:mm:yy format.`	The following types of text content are set off with a special font: • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

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

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 solve an arisen issue on your own, we recommend that you contact the Technical Support Service at Kaspersky Lab (see section "Technical support by phone" on page 80).

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

The application's page at the Kaspersky Lab website

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

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

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

The application's Knowledge Base page at the Technical Support Service website

Knowledge Base is a section of the Technical Support Service website that provides recommendations on how to work with 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.

Context help provides information about each window of the application, listing and describing the corresponding settings and a list of tasks.

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

Documentation

The application delivery set includes documents that will help you install and activate the application on computers in a local area network, configure application settings, and learn the basic principles of 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 Writing and Localization Unit. For example, if you would like to leave feedback.

KASPERSKY SECURITY CENTER

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

Kaspersky Security Center is designed for centralized execution of basic administration and maintenance tasks in an organization's network. The application provides the administrator 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 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 providers*).

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.

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

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

- Receive statistics and reports about the operation of applications and devices.

- Receive notifications about critical events in the operation of Kaspersky Lab applications.

- 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 basic components:

- **Administration Server** (hereinafter also referred to as *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 to Administration Server and Kaspersky Security Center Web-Console

COMPONENT	REQUIREMENTS
Operating system	Microsoft® Windows XP Professional with Service Pack 2 or later installed Microsoft Windows XP Professional x64 or later; Microsoft Windows Vista® Service Pack 1 or later; Microsoft Windows Vista x64 Service Pack 1 with all current updates installed (Microsoft Windows Installer 4.5 must be installed for Microsoft Windows Vista x64); Microsoft Windows 7; Microsoft Windows 7 x64; Microsoft Windows 8; Microsoft Windows 8 x64; Microsoft Windows Server 2003 or later; Microsoft Windows Server 2003 x64 or later; Microsoft Windows Server 2008; Microsoft Windows Server 2008 deployed in Server Core mode; Microsoft Windows Server 2008 x64 Service Pack 1 with all current updates installed (Microsoft Windows Installer 4.5 must be installed for Microsoft Windows Server 2008 x64); Microsoft Windows Server 2008 R2; Microsoft Windows Server 2008 R2 deployed in Server Core mode; Microsoft Windows Server 2012.
Data Access Components	Microsoft Data Access Components (MDAC) 2.8 or later; Microsoft Windows DAC 6.0.
Database Management System	Microsoft SQL Server® Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2008 R2, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, MySQL versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091; MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.

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

OPERATING SYSTEM	CPU FREQUENCY, GHZ	RAM SIZE, GB	AVAILABLE DISK SPACE, GB
Microsoft Windows, 32-bit	1 or higher	4	10
Microsoft Windows, 64-bit	1.4 or higher	4	10

Administration Console

Table 4. Software requirements to Administration Console

COMPONENT	REQUIREMENTS
Operating system	Microsoft Windows (supported version of the operating system is determined by the requirements of Administration Server).
Management Console	Microsoft Management Console 2.0 or later.
Browser	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 working with Microsoft Windows 7; Microsoft Internet Explorer 10.0 or later when working with Microsoft Windows 8.

Table 5. Hardware requirements to Administration Console

OPERATING SYSTEM	CPU FREQUENCY, GHZ	RAM SIZE, MB	AVAILABLE DISK SPACE, GB
Microsoft Windows, 32-bit	1 or higher	512	1
Microsoft Windows, 64-bit	1.4 or higher	512	1

When using the Systems Management functionality, you should have at least 100 GB free disk size.

iOS Mobile Device Management mobile devices server

Table 6. Software requirements to the iOS MDM mobile devices server

COMPONENT	REQUIREMENTS
Operating system	Microsoft Windows (supported version of the operating system is determined by the requirements of Administration Server).

Table 7. Hardware requirements to the iOS MDM mobile devices server

OPERATING SYSTEM	CPU FREQUENCY, GHZ	RAM SIZE, GB	AVAILABLE DISK SPACE, GB
Microsoft Windows, 32-bit	1 or higher	2	2
Microsoft Windows, 64-bit	1.4 or higher	2	2

Mobile devices server supporting Exchange ActiveSync

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

Network Agent or Update Agent

Table 8. Software requirements to Network Agent and Update Agent

COMPONENT	REQUIREMENTS
Operating system	Microsoft Windows; Linux®; Mac OS.

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

Table 9. Hardware requirements to Network Agent and Update Agent

OPERATING SYSTEM	CPU FREQUENCY, GHZ	RAM SIZE, GB	FREE DISK SPACE AVAILABLE FOR NETWORK AGENT, GB	FREE DISK SPACE AVAILABLE FOR UPDATE AGENT, GB
Microsoft Windows, 32-bit	1 or higher	0.5	1	4
Microsoft Windows, 64-bit	1.4 or higher	0.5	1	4
Linux, 32-bit	1 or higher	1	1	4
Linux, 64-bit	1.4 or higher	1	1	4
Mac OS	1	1	1	4

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

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

Table 11. Summarized results of Administration Server performance testing under a 64-bit operating system

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

If you connect Administration Server to MySQL and SQL Express database server, it is not recommended to use application to manage more than 5000 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 the information from items 1 and 2, as well as data from administration system loading tests (see section "Network load" on page 75). 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 schemes of protection system deployment on an enterprise network using Kaspersky Security Center.

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

- Deploying a protection system via Kaspersky Security Center, using one of the following methods:
  - by using the Administration Console
  - through 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 details refer to the full Help of Kaspersky Security Center.

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

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

1. The administrator deploys the Administration Server as follows:
    a. installs Kaspersky Security Center on the 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 TOOLS WITHIN AN ORGANIZATION

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

1. The administrator deploys the Administration Server as follows:

   a. installs Kaspersky Security Center on the selected computer;

   b. installs Kaspersky Security Center Web-Console on 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 creates a virtual Administration Server in Kaspersky Security Center in order to manage client computers.

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 creates and configures installation packages of Network Agent and required Kaspersky Lab applications.

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

6. In Kaspersky Security Center Web-Console the administrator starts installation of selected applications on client computers.

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

DEPLOYING A PROTECTION SYSTEM MANUALLY WITHIN AN ORGANIZATION

Manual installation of required software with 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 on the 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

Remote installation of required software through Kaspersky Security Center Web-Console is performed 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 the Administration Server as follows:
   a. installs Kaspersky Security Center on the selected computer;
   b. installs Kaspersky Security Center Web-Console on 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 Kaspersky Security Center administrator creates a virtual Administration Server in Kaspersky Security Center in order to manage client computers.
3. The administrator of Kaspersky Security Center 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 Kaspersky Security Center administrator creates and configures installation packages of the Network Agent and Kaspersky Lab required applications.
5. The administrator of Kaspersky Security Center selects computers from the Administration Console to which they want to install the required application.
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 TOOLS ON A CLIENT ORGANIZATION'S NETWORK

Remote installation of required software through Kaspersky Security Center Web-Console is performed 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 the Administration Server as follows:

   a. installs Kaspersky Security Center on the selected computer;

   b. installs Kaspersky Security Center Web-Console on 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 Kaspersky Security Center administrator creates a virtual Administration Server in Kaspersky Security Center in order to manage client computers.

3. The administrator of the client enterprise 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 Kaspersky Security Center administrator creates and configures installation packages of the Network Agent and Kaspersky Lab required 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 through the Administration Console, using policies and local settings of applications.

DEPLOYING A PROTECTION SYSTEM ON A CLIENT ORGANIZATION'S NETWORK MANUALLY

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

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

   a. installs Kaspersky Security Center on the selected computer;

   b. installs Kaspersky Security Center Web-Console on 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 Kaspersky Security Center administrator creates a virtual Administration Server in Kaspersky Security Center in order to manage client computers.

3. The administrator of the client enterprise 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 Kaspersky Security Center administrator creates and configures installation packages of the Network Agent and Kaspersky Lab required applications.

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

6. Kaspersky Security Center administrator sends the stand-alone 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 stand-alone package to the selected computers through Kaspersky Security Center Web-Console.

8. Users of client computers start application installation by using a stand-alone 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 to manage client computer access to network. To ensure the system health when both Kaspersky Security Center and Microsoft NAP are running, you should install the System Health Validator component (see section "Installing and configuring Kaspersky Security Center SHV" on page 39).

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

IN THIS SECTION

STAGES OF DEPLOYING ADMINISTRATION SERVER WITHIN AN ENTERPRISE

To deploy Administration Server within an organization:

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

UPGRADING A PREVIOUS VERSION OF KASPERSKY SECURITY CENTER

You can install Administration Server 10.0 to a computer where the previous version of Administration Server is installed. When you upgrade Administration Server to version 10.0, all data and settings from the previous version of the application are saved.

To upgrade Administration Server of the 9.0 version to the 10.0 version:

1. Run the executable file setup.exe for the version 10.0.

   The Setup Wizard starts, which prompts you to create a backup copy of Administration Server data for Kaspersky Security Center 9.0.

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

2. 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 using klbackup utility. This utility is included in the application distribution kit, being 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.

3. Install Administration Server version 10.0, followinf the Setup Wizard's instructions.

   Aborting the upgrading process at the step of Administration Server installation may cause inoperability of Kaspersky Security Center 9.0.

4. For computers on which the previous version of Network Agent has been installed, create and run the Network Agent new version remote installation task (see section "Installing applications using a remote installation task" on page 49).

   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:

- **Typical**. 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 on a network, you can install Servers to other computers on the same network using the remote installation task, involving the method of forced installation (see section "Installing applications using a remote installation task" on page 49). When creating the remote installation task, you should use the Administration Server installation package.

IN THIS SECTION

INSTALLATION PREPARATION

Before launching installation, make sure that the computer hardware and software meets the requirements for Administration Server and Administration Console (see section "Hardware and software requirements" on page 14).

Kaspersky Security Center stores its information in a SQL Server database. By default, Microsoft SQL Server 2008 R2 Express Edition is installed together with Kaspersky Security Center for that purpose. Other SQL servers (see section "Hardware and software requirements" on page 14) can be used for storing data. In that case they must be installed on the network before the start of installation of Kaspersky Security Center.

Installation of Kaspersky Security Center requires administrator privileges on the computer where 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 table below).

Table 12. Ports used by Kaspersky Security Center

PORT NUMBER	PROTOCOL	DESCRIPTION
Computer on which the Administration Server is installed		
8060	HTTP	Used for connection to Web Server for the operation of Kaspersky Security Center Web-Console and organization of the enterprise's intranet.
8061	HTTPS	Used for connection to Web Server for the operation of Kaspersky Security Center Web-Console and organization of the enterprise's intranet. Connection presumes encryption.
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 connection to a KSN server.
13291	TCP	Used for connection of Administration Console to Administration Server. SSL protection is used for these connections.
13292	TCP	The port is used for connection of 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.
17000	TCP	Used for connection to an activation proxy server. SSL protection is used for these connections.
17100	TCP	Used for connection to an activation proxy server in order to activate mobile clients.
18000	HTTP	Administration Server uses this port to receive data from the Cisco® NAC authentication server.
Computer designated as Update Agent		
13000	TCP	The port is used by client computers to connect to the Update Agent.
13001	TCP	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.
14000	TCP	The port is used by client computers to connect to the Update Agent.
14001	TCP	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.
Client computer with Network Agent installed		
7	UDP	The port is used by the Wake On LAN feature.
67	UDP	Used on a computer that has been assigned to be the PXE server when deploying operating system images.
69	UDP	

PORT NUMBER	PROTOCOL	DESCRIPTION
15000	UDP	The port is used to receive requests for connection to the Administration Server, which can collect information about a host computer in real time.
15001	UDP	Used to interact with Update Agent.

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 Server 2008 the default range of ports for outbound connections is 49152–65535 (TCP).

TYPICAL INSTALLATION

To perform Kaspersky Security Center standard installation on a local computer:

1. Run the setup.exe file. The Setup Wizard will offer you to adjust the application settings. Follow the wizard's instructions.
2. Read the License Agreement thoroughly. If you accept all of its terms, select the **I accept the terms of the License Agreement** check box. The installation will proceed.
3. Select **Typical** and click the **Next** button.

Then 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. At the first startup of the Console you can perform the initial configuration of the application (for details refer to the *Administrator's Guide of Kaspersky Security Center*).

When the Setup Wizard completes its operation, 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 will also be installed, if they were not installed earlier:

- 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 a custom installation of Kaspersky Security Center on a local computer:

Run the setup.exe file.

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

Further items describe steps of the Setup Wizard and actions that you can perform at each of those steps.

STEPS OF THE WIZARD

STEP 1. REVIEWING THE LICENSE AGREEMENT

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

Read the License Agreement thoroughly. If you accept all of its terms, select the **I accept the terms of the License Agreement** check box. The installation will proceed.

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

STEP 2. SELECTING THE INSTALLATION TYPE

Select the **Custom** installation method.

STEP 3. SELECTING THE COMPONENTS TO BE INSTALLED

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

- **Kaspersky Lab Cisco NAC Posture Validation Server**. This is a standard Kaspersky Lab component authorizing a set of credentials for common operation with Cisco NAC. The settings of 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 protection management of mobile devices through Kaspersky Security Center.

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

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

The Wizard dialog box contains reference information about the selected component and the disk space required for its 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 will be 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 restart the installation of Administration Server.

At this step you should 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 such folder does not exist, it will be created automatically during the installation. You can change the destination folder by using the **Browse** button.

STEP 4. SELECTING NETWORK SCALE

Specify the scale of the network on which Kaspersky Security Center is installed. Depending on the number of computers on the network, the Wizard configures installation and appearance of the application interface.

The table below lists application installation settings and interface appearance settings, depending on various network scales.

Table 13. Dependence of installation settings on the network scale selected

SETTINGS	1 TO 100 COMPUTERS	100 TO 1.000 COMPUTERS	1.000 TO 5.000 COMPUTERS	5.000+ COMPUTERS
Displaying the node of slave and virtual Administration Servers and all settings related to slave and virtual Administration Servers in the console tree	not available	not available	available	available
Displaying the **Security** sections in the properties windows of the Administration Server and administration groups	not available	not available	available	available
Creating a Network Agent policy using the Quick Start Wizard	not available	not available	available	available
Random distribution of startup time for the update task on client computers	not available	in interval of 5 minutes	in interval of 10 minutes	in interval of 10 minutes

If you connect Administration Server to MySQL and SQL Express database server, it is not recommended to use application to manage more than 5000 computers.

STEP 5. SELECTING THE ACCOUNT

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

- **Local System Account**. Administration Server will start under the *Local System Account* and using its credentials.

  Correct operation of Kaspersky Security Center requires that the account used to start the Administration Server had the rights of administrator of the resource where the Administration Server database is hosted.

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

- **User account**. Administration Server will start using the user account. Administration Server will initiate all operations by using the credentials of that account. Use the **Browse** button to select the user whose account will be used and enter the password.

When using an SQL server in a mode that presupposes authenticating user accounts with Microsoft Windows tools, access to the database should be granted. The user account should be assigned the status of owner of Kaspersky Anti-Virus database. The dbo scheme 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 detailed information refer to the *Kaspersky Security Center Administrator's Guide*.

STEP 6. SELECTING THE DATABASE

At this step of the Wizard you should select a resource – Microsoft SQL Server (SQL Express) or MySQL – that will be used to store the Administration Server information 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 klakdb.chm file, 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 selected, the following options of SQL server configuration are available:

- If you have selected SQL Express or Microsoft SQL Server at 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 where Kaspersky Security Center is being installed. Clicking the **Browse** button displays a list of all SQL Servers installed in the network.

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

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

If you plan to manage fewer than 5000 computers with Kaspersky Security Center, Microsoft SQL Express 2005 / 2008 can be used. If the planned number of computers managed with Kaspersky Security Center exceeds 5 000, Microsoft SQL 2005 / 2008 is recommended.

- If no SQL Server is installed on the organization's network, select **Install Microsoft SQL Server 2008 R2 Express Edition**.

  The Setup Wizard will then install Microsoft SQL Server 2008 R2 Express Edition. The necessary settings will be 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). Specify the port for connection in the **Port** field (the default port number is 3306).

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

If you want to install an SQL Server manually on the computer from which you initiate installation of Kaspersky Security Center, you must terminate the installation and restart it after SQL Server installation. The supported SQL servers are listed in the system requirements (see section "Hardware and software requirements" on page 14).

If you are installing the server on a remote computer, there is no need to interrupt the Kaspersky Security Center Setup Wizard. Install the SQL Server and resume Kaspersky Security Center installation.

STEP 8. SELECTING THE AUTHENTICATION MODE

Determine the authentication mode that will be used during the Administration Server connection to the SQL Server.

Depending on the selected database, 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**. To verify rights, the account for starting Administration Server will be used.

  - **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 the SQL Server authentication mode when installing or upgrading the Administration Server. This may occur when the computer storing the database is outside the domain or when the Administration Server is installed under the 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 (the files are copied to Administration Server during creation of installation packages).

- Store updates downloaded from an update source to the Administration Server.

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

You can select either of the following options:

- **Create a shared folder**. Creating a new folder. Specify the path to folder in the field below.
- **Select existing shared folder**. Selecting a shared folder from among existing folders.

The shared folder can be a local folder on the computer running the installer or remote directory on any client computer in the corporate network. You can use the **Browse** button to select the shared folder or specify it manually by entering its UNC path (for example, \\server\KLSHARE) in the corresponding field.

By default, the installer creates a local subfolder named KLSHARE in the folder selected for installation of Kaspersky Security Center components.

STEP 10. CONFIGURING CONNECTION TO ADMINISTRATION SERVER

Configure connection to Administration Server:

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

If Administration Server is installed on a computer running under Microsoft Windows XP with Service Pack 2, the built-in system firewall blocks TCP ports 13000 and 14000. Therefore, to allow access to the computer with Administration Server installed, 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 in 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 virtual Administration Server, the address specified on this wizard step is used as master Administration Server address by default.

STEP 12. CONFIGURING THE SETTINGS FOR MOBILE DEVICES

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

Specify the Administration Server address for connection of mobile devices.

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 virtual Administration Server, the address specified on this wizard step is used as master Administration Server address by default.

STEP 13. SELECTING APPLICATION CONTROL PLUGINS

Select application management plug-ins that should be installed with Kaspersky Security Center.

STEP 14. COMPLETING INSTALLATION

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

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

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 will be 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.

Kaspersky Lab's Posture Validation Server service for Cisco NAC will apply on the computer if Kaspersky Lab Cisco NAC Posture Validation Server has been installed together with Administration Server.

Table 14. Service attributes

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

The server version of Network Agent will be installed on the 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 configure the connection of Network Agent to Administration Server; the configuration is implemented programmatically because the components are 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 with 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 a 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 <Drive>:\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 assumes that the network includes a dedicated server with Microsoft Windows Server 2008 installed running the Posture Validation Server (PVS), and that client computers have NAP-compatible operating systems installed: Microsoft Windows Vista, Microsoft Windows XP with Service Pack 3, or Microsoft Windows 7.

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

To install Kaspersky Security Center to a computer locally:

1. Run the setup.exe file from the CD containing the distribution of the Kaspersky Security Center SHV.

   This will start the Setup Wizard. Follow the wizard's instructions.

   The installation of Kaspersky Security Center SHV from the distribution downloaded from the Internet does not differ from the installation that is done with the installation CD.

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

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

After the Wizard completes, the 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 on a local computer,

run the setup.exe file from the CD containing the distribution 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 downloaded from the Internet does not differ from the installation that is done with the installation CD.

STEPS OF THE WIZARD

STEP 1. REVIEWING THE LICENSE AGREEMENT

At this stage 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 on Linux platform, you should have a license for Kaspersky Security Center Web-Console, Service Provider Edition.

Read the License Agreement thoroughly. If you accept all of its terms, select the **I accept the terms of the License Agreement** check box. The installation will proceed.

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

Kaspersky Security Center Web-Console remote installation using an installation package or local installation in non-interactive mode means automatic acceptance of the terms of the License Agreement related to the application that you are installing. You can view the License Agreement for a specific application in the distribution kit of that application or on the website of Kaspersky Lab Technical Support.

STEP 2. SELECTING THE DESTINATION FOLDER

Select 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 way 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 on the remote computer. If this option is selected, the Setup Wizard proceeds to the Step 7 (see section "Step 7. Starting the installation of Kaspersky Security Center Web-Console" on page 42).

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-9.<build_number>.i386.rpm;
  - kscwebconsole_9.<build_number>_i386.deb.
- For 64-bit systems:
  - kscwebconsole-9.<build_number>.x86_64.rpm;
  - kscwebconsole_9.<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 available methods:
  - **Select certificate file.** You can select an existing certificate by clicking the **Browse** button.
  - **Select a private key**. You can specify a certificate using the file of its closed key by clicking the **Browse** button.

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 THE INSTALLATION OF KASPERSKY SECURITY CENTER WEB-CONSOLE

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

The installation process is displayed on the Wizard page.

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

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

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

CONFIGURING THE OPERATION OF THE ADMINISTRATION SERVER WITH 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 or Kaspersky Security Center 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 sever administrator account from among the accounts offered by the application or create a new account. Under this account the administrator of the corporate network managed by the selected virtual Administration Server starts Kaspersky Security Center Web-Console to view the anti-virus protection 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:

   - Address of the server where Kaspersky Security Center Web-Console is installed (in the form of an URL address 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
   - Resolution: 220×72 pixels.

2. Place the logo file to the installation folder of the Apache server.

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

For more details on how to configure the cooperation between Administration Server and Kaspersky Security Center Web-Console refer to the *Administrator's Guide of Kaspersky Security Center*.

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 (see page 48) section.

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

IN THIS SECTION

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 next time it scans the network, moving it to the **Unassigned computers** folder. Because the Update Agent is Firewall-protected, 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 structure is used for the virtual Server address: **<Full address of physical Administration Server to which the virtual Server belongs>/<Name of 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 62

Remote deployment of applications 48

REQUIREMENTS TO INSTALLATION OF APPLICATIONS ON COMPUTERS OF A CLIENT ENTERPRISE

Remote installation of applications to computers of a client organization is the same as that within an enterprise (see section "Remote installation of software (see page 48)").

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 AN 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 described 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 DEPLOYMENT OF APPLICATIONS

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

Before deploying applications on client computers, make sure that the hardware and software of client computers meets the applicable requirements (see section "Hardware and software requirements" on page 14).

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 plugins. 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). 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 deployment of an application has ended in an error, you can check what caused this error and fix it using the remote deployment preparation utility (see section "Preparing computer for remote installation. The riprep.exe utility" on page 58).

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

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 are opened automatically by the remote deployment preparation utility (see section "Preparing computer for remote installation. The riprep.exe utility" on page 58).

IN THIS SECTION

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 tasks 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 makes it possible to install Kaspersky Lab applications using Active Directory group policies.

The installation of applications using Active Directory group policies is possible only with installation packages comprising 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 contains client computers to which the task is deployed. 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 is missing from any of the slave Servers, distribute it using the installation package distribution task (see section "Distributing installation packages to slave Administration Servers" on page 56).
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 slave Administration Servers in the selected administration group, launch the creation of a remote deployment group task for this group (see section "Installing an application on client computers in the administration group" on page 50).
   - If you want to create a task for specific slave Administration Serves, launch the creation of a remote deployment task for specific computers (see section "Installing an application on specific client computers" on page 50).

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

   In the **Task type** window of the Net Task Wizard in the **Kaspersky Security Center Administration Server** section, open the **Advanced** folder and select the task **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 specifically created installation packages or directly from distributions.

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 within the domain. They are opened automatically by using the utility for remote deployment preparation. (see section "Preparing computer for remote installation. The riprep.exe utility" on page 58)

To install an application using the Remote Setup 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 the name, which corresponds the application's name and version. You can use this installation package to install the application subsequently.

- 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: **Deploy <Name of the installation package>**.

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 REMOVAL OF APPLICATIONS

Using Kaspersky Security Center, you can remove incompatible applications that can cause conflicts in the operation of Kaspersky Lab software managed through 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

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 uninstall an application remotely from specified 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 tasks 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 the same installation package many 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

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.

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, you can create it again by selecting the nagent9.kud file in the NetAgent folder of the Kaspersky Security Center distribution package.

When creating an Administration Server installation package, select the sc9.kud file in the root folder of the Kaspersky Security Center distribution package as the description file.

DISTRIBUTING INSTALLATION PACKAGES TO SLAVE ADMINISTRATION SERVERS

To distribute installation packages to slave Administration Servers:

1. Establish a connection with the Administration Server that controls the relevant slave Administration Servers.
2. Start the creation of a task of installation package distribution to slave Administration Servers in one of the following ways:
   - If you want to create a task for slave Administration Servers in the selected administration group, launch the creation of a group task for this group.
   - If you want to create a task for specific slave Administration Serves, 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 Net Task Wizard in the **Kaspersky Security Center Administration Server** node, open the **Advanced** folder and select the **Distribute installation package** task.

   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 DEPLOYMENT 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.

The information about the results of installation of the user-defined application will be registered in the logs of Kaspersky Security Center, and it will appear in the list of events, in the reports and task 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 retrieving up-to-date versions of corporate applications by Kaspersky Lab:

1. Open the main application 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** line.

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

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

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

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

SEE ALSO:

PREPARING COMPUTER FOR REMOTE INSTALLATION. THE RIPREP.EXE UTILITY

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

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 (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 forcedly.
- 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 a 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;
- Kaspersky Security for Virtualization 1.1.

IN THIS SECTION

LOCAL INSTALLATION OF NETWORK AGENT

To install Network Agent on a computer locally,

run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center in the Packages\NetAgent folder. This starts the Network Agent Setup Wizard. Follow the wizard's instructions.

The installation of Network Agent from the distribution package downloaded from the Internet does not differ from the installation from the installation CD.

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.

If you want to use a computer on which Network Agent is installed as a connection gateway for a selected administration group, you should specify that the computer on which the Network Agent is installed is the Update Agent for that group, being used as a connection gateway (see section "Defining an Update Agent. Configuring Update Agent" on page 44).

Network Agent remote installation using an installation package or local installation in non-interactive mode means automatic acceptance of the terms of the License Agreement related to the application that you are installing. You can view the License Agreement for a specific application in the distribution kit of that application or on the website of Kaspersky Lab Technical Support.

LOCAL INSTALLATION OF THE APPLICATION 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 SILENT MODE

To install an application in silent mode:

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

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

3. Open the folder storing the required installation package in one of the following ways:

   - Copy the folder corresponding to the relevant installation package from the Administration Server to the client 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 the Microsoft Windows Vista operating system, select the **Disabled** value for the setting **User Account Control: Run all administrators in Admin Approval Mode** (**Start** → **Control Panel** → **Administration** → **Local security policy** → **Security settings**).

4. Depending on the application selected, perform the following actions:

   - in the case of Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers and Kaspersky Security Center, open the exec subfolder and run the executable file (a file with the .exe extension) with the /s key.

   - in the case of other Kaspersky Lab applications, run the executable file (a file with the .exe extension) with the /s key in the open folder.

Running the executable file with the key `EULA=1` means that you have accepted the terms of the License Agreement. The text of the License Agreement is included in the distribution kit of Kaspersky Security Center. Accepting the terms of the License Agreement is necessary for installing or upgrading the application.

INSTALLING SOFTWARE BY USING STAND-ALONE PACKAGES

Kaspersky Security Center allows creating stand-alone packages for installation of applications. A stand-alone package is an executable file that can be located on the web server, sent by email, or transferred to client in other way. You can start the received file locally on the computer and install the application, without Kaspersky Security Center participation.

To install an application using stand-alone installation package:

1. Connect to the necessary Administration Server.

2. In the **Remote installation** folder of the console tree select the **Installation packages** subfolder.

3. In the workspace, select the installation package of the required application.

4. Launch the process of creating a stand-alone installation package using one of the following methods:

   - in the context menu of the installation package, select **Create stand-alone installation package**;

   - click the **Create stand-alone installation package** 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 for transmitting the stand-alone installation package to a client computer.

5. Transmit the stand-alone installation package to the client computer.

6. Run the stand-alone installation package on the client computer.

As a result, the application will be installed on the client computer with the settings specified in the stand-alone installation package.

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 and running under the following operating systems:

- Windows Mobile
- Windows CE
- Windows Phone 7
- Android™;
- Symbian;
- Bada;
- Apple iOS.

IN THIS SECTION

MOBILE DEVICES SERVERS

Gathering information about mobile devices and storing their profiles are provided by Mobile devices servers. A *mobile devices server* is a component of Kaspersky Security Center that provides the administrator access to mobile devices and allows managing them via 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:

- An individual mobile device
- Several mobile devices
- 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 ActiveSync protocol.

The following operating systems support ActiveSync protocol:

- Windows Mobile
- Windows CE
- Windows Phone 7
- Android
- Symbian;
- Bada.

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.
2. 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.
3. The 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.
4. 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 devices that have been connected. For details on how to manage Exchange ActiveSync mobile devices, refer to the Kaspersky Security Center Administrator's Guide.

IN THIS SECTION

INSTALLING A MOBILE DEVICES SERVER FOR EXCHANGE ACTIVESYNC

To install a mobile devices server for Exchange ActiveSync:

1. In the Kaspersky Security Center installation package in the MDM4Exchange folder run the installation file named setup.
2. Follow the Setup Wizard's instructions.

CREATING A MANAGEMENT PROFILE FOR EXCHANGE ACTIVESYNC DEVICES

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 settngs 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.
9. If you want the newly created profile to be the default one, select it 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. Any iOS mobile devices connected to an iOS MDM mobile devices server and managed by Administration Server, are called *iOS MDM mobile devices.* Connection of iOS MDM mobile devices 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 installs an Apple Push Notification Service (APNs) certificate to Administration Server.
3. The administrator sends the iOS mobile device user a URL for downloading an iOS MDM profile (see section "Installing an iOS MDM profile to iOS mobile device" on page 69). An *iOS MDM profile* is used for connecting iOS MDM mobile devices to an iOS MDM mobile devices server.
4. The user installs the iOS MDM profile to the iOS mobile device:
5. The mobile devices connects to iOS MDM mobile devices server. Connected iOS MDM mobile devices are displayed in the **iOS MDM mobile devices** folder contained in the **Mobile devices** folder of the console tree.

For details 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:

1. In the installation package of Kaspersky Security Center in the MDM4iOS folder run the installation file named setup.

   The iOS MDM Administration Server Installation Wizard starts.

2. In the **Settings for connection to iOS MDM mobile devices server** window of the Wizard adjust 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.
   - **Local 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.
   - **External port to connect to iOS MDM service**. In this field specify an external port for connection of mobile devices to the iOS MDM service. The default port number is 443.

   It is recommended to use default values.

3. In the **Select certificate** window of the Wizard, select a certificate that will be used when iOS MDM Mobile Devices Server to Administration Server:

   - **Create** button. Select this option if you want to create a new certificate. In the **URL of remote connection with Mobile devices server** field, enter the address of a client computer to which Mobile devices server will be installed. This client computer should be available for connection of iOS MDM mobile devices.
   - **Select certificate file**. Select this option if you want to use an existing certificate. In the **Path to file** field specify the path to the certificate file.

After the Wizard completes its operations, the iOS MDM mobile devices server is installed to the local client computer.

RECEIVING AN APNS CERTIFICATE

To receive an APNs certificate:

1. Create a request for an APNs certificate in the Internet Information Services (IIS).
2. Register a key for iOS MDM mobile devices server in My Kaspersky Account on the Kaspersky Lab website.

   After the registration, the **Sign a request for a certificate** link becomes available

3. Request certificate signature in My Kaspersky Account on the Kaspersky Lab website by clicking the **Sign certificate request** link.

   When a signed request will be ready, you will receive a notification.

4. Download the signed request from Kaspersky Lab website.
5. Upload the signed request for certificate to the Apple Inc. website using 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.

6. Download an APNs certificate from the Apple Inc. website.

INSTALLING AN APNS CERTIFICATE TO AN 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** block of settings click the **Install** button.

The APNs certificate will be installed.

INSTALLING AN IOS MDM PROFILE TO IOS MOBILE DEVICE

To install an iOS MDM profile 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. In the **iOS MDM profile installation** window specify how to notify user upon the installation of iOS MDM profile to mobile device:

   - **By SMS**. Select the check box if you want to send the MDM profile link by SMS. In the **SMS text** field enter a message for the user or use the default one. From the drop-down list next to the **SMS text** entry field select **One-off password** and specify user password.
   - **Email**. Select the check box to send the user an email notification containing a URL for downloading the MDM profile and also containing a dedicated QR code. In the **Subject** field enter the message subject. In the **Notification message** field enter a message for the user. From the drop-down list next to the **SMS text** entry field select **One-off password** and specify user password.
6. Click **OK**.

As a result, the mobile device user receives a notification with a link for iOS MDM profile download from website. The user then installs iOS MDM profile to iOS device.

ADDING A CONFIGURATION PROFILE TO AN IOS MDM MOBILE DEVICES SERVER

To add a configuration profile 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 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 application named iPhone Configuration Utility should be installed on the computer to allow you to create a configuration profile. The application is installed using standard Windows tools.

The added configuration profile is displayed in the **Profiles** section of the properties window of the iOS MDM mobile devices server.

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 mobie 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

To add a provisioning profile to iOS MDM mobile devices server:

1. Create provisioning profiles on Apple Inc. web portal in iOS Dev Center.
2. In the **Managing mobile devices** folder of the console tree select the **Mobile devices servers** subfolder.
3. In the workspace of the **Mobile devices servers** folder select an iOS MDM mobile devices server.
4. Select **Properties** from the context menu of the iOS MDM Mobile devices server.

   The Mobile devices server properties window opens.
5. 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

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: Reports and notifications** window opens.

2. In the **Properties: Reports and notifications** window select the **SMS senders** section.

3. Click the **Add** button in the **SMS senders** section.

   The **Select device** window opens.

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

INITIAL DEPLOYMENT OF ANTI-VIRUS PROTECTION

This section provides information about traffic volume values after Network Agent 10.0 and Kaspersky Endpoint Security 8 for Windows are installed to the client computer (see the table below).

The Network Agent is installed using push install, when the files required for setup are copied by the Administration Server to a shared folder on the client computer. After installation, the Network Agent retrieves the distribution package of Kaspersky Endpoint Security 8 for Windows using connection to the Administration Server.

Table 15. Traffic

SCENARIO	NETWORK AGENT INSTALLATION FOR A SINGLE CLIENT COMPUTER	INSTALLING KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS TO ONE CLIENT COMPUTER (WITH DATABASES UPDATED)	CONCURRENT INSTALLATION OF THE NETWORK AGENT AND KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS
Traffic from client computer to Administration Server, kB	386.70	1 841.3	2 253.8
Traffic from Administration Server to client computer, KB	14 801.13	269 994.5	284 768.7
Total traffic (for a single client computer), KB	15 187.83	271 835.8	287 022.5

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 16. Traffic

SCENARIO	INITIAL UPDATE OF THE ANTI-VIRUS DATABASES[1]
Traffic from client computer to Administration Server, kB	1 357.1
Traffic from Administration Server to client computer, KB	33 917.0
Total traffic (for a single client computer), KB	35 274.1

SYNCHRONIZING A CLIENT WITH THE ADMINISTRATION SERVER

This scenario describes the state of the administration system when intensive data synchronization occurs between a client 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 17. Traffic

SCENARIO	Traffic from client computers to Administration Server, kB	Traffic from Administration Server to client computers, kB	Total traffic (for a single client computer), KB[2]
INITIAL SYNCHRONIZATION[3] PRIOR TO UPDATING DATABASES ON A CLIENT COMPUTER	368.6	463.7	832.3
INITIAL SYNCHRONIZATION[4] AFTER UPDATING DATABASES ON A CLIENT COMPUTER	1 748.3	34 388.3	36 136.6
SYNCHRONIZATION WITH NO CHANGES ON A CLIENT COMPUTER AND THE ADMINISTRATION SERVER	8.7	6.6	15.3
SYNCHRONIZATION AFTER CHANGING THE VALUE OF A SETTING IN A GROUP POLICY[5]	11.1	13.3	24.4
SYNCHRONIZATION AFTER CHANGING THE VALUE OF A SETTING IN A GROUP TASK	10.0	12.5	22.5
FORCED SYNCHRONIZATION WITH NO CHANGES ON A CLIENT COMPUTER	47.3	15.5	62.8

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 18. Traffic

SCENARIO	INCREMENTAL UPDATE OF ANTI-VIRUS DATABASES[6]
Traffic from client computer to Administration Server, kB	436.9
Traffic from Administration Server to client computer, KB	9 979.2
Total traffic (for a single client computer), KB[7]	10 416.1

[2] 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 Nstands for the total number of computers included in the administration group.
[3] 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.
[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] 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.
[6] The data in the table may vary slightly depending upon the current anti-virus database version.
[7] 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 Nstands 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 19. Traffic

SCENARIO[8]	DATA TRANSFER TO ADMINISTRATION SERVER UPON A "VIRUS DETECTED" EVENT	DATA TRANSFER TO ADMINISTRATION SERVER UPON NINE "VIRUS DETECTED" EVENTS
Traffic from client computer to Administration Server, kB	27.2	100.4
Traffic from Administration Server to client computer, KB	25.8	52.5
Total traffic (for a single client computer), KB	53.0	152.9

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 20. Traffic

SCENARIO	"IDLE" STATE OF THE ADMINISTRATION SYSTEM[9]
Traffic from client computer to Administration Server, kB	2 922.1
Traffic from Administration Server to client computer, KB	15 140.5
Total traffic (for a single client computer), KB	18 062.6

[8] 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 Serverwas 20 minutes, updates were downloaded to the Administration Server storageonce 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.

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

Table 21. Rate of database filling with events

NUMBER OF DEVICES WHERE MANAGED APPLICATIONS ARE INSTALLED	NUMBER OF EVENTS ADDED TO THE DATABASE PER DAY
100	≤ 2,000
1,000	≤ 20,000
10,000	≤ 200,000

The table contains data for standard run mode of managed applications allowing not more than 20 events per day to be received from each client device.

The maximum number of events stored in the database is defined in the **Settings** section of the properties window of Administration Server. By default, the database contains not more than 400 000 events.

CONTACTING TECHNICAL SUPPORT

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

IN THIS SECTION

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 (on page 10), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support Service specialists will answer any of your questions about installing and using the application.

Before contacting Technical Support, please read 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.
- Sending a request via Kaspersky CompanyAccount system on the website of Technical Support Service. 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/support/international) by phone.

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/details). 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 gain access to Kaspersky CompanyAccount, you should register on the registration page (https://support.kaspersky.com/companyaccount/registration) and receive a login and a 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 Service in Russian, English, 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 text.

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 of the following types to the Virus Lab:

- *Unknown malicious program* – you suspect that a file contains a virus, but Kaspersky Security Center has not identified the file as infected.

  Virus Lab specialists analyze malicious code sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- *False alarm* – Kaspersky Security Center classifies the file as a virus, while you are sure that the file contains no viruses.

You can also send requests to the Virus Lab from the page with the request form (http://support.kaspersky.com/virlab/helpdesk.html) without registering in Kaspersky CompanyAccount. On this page, 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

A

Active key

Key that is used at the moment for application operation.

Additional key

Key that verifies the right to use the application but is not used at the moment.

Administration Console

A Kaspersky Security Center component that provides a user interface for the administrative services of Administration Server and Network Agent.

Administration group

A set of computers that share common functions and a set of Kaspersky Lab applications that is installed on them. Computers are grouped so that they can be managed conveniently as a single unit. A group may include other groups. It is possible to create group policies and group tasks for each installed application in the group.

Administration Server

A component of Kaspersky Security Center that centralizes the storage of information about Kaspersky Lab applications installed on the corporate network and about the management of those applications.

Administration Server certificate

A certificate which allows Administration Server authentication when connecting the Administration Console to it and when exchanging data with users' 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 Sever (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

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 that can be managed through Kaspersky Security Center SPE has its own plug-in. It is included in all Kaspersky Lab applications that can be managed by using Kaspersky Security Center.

APPLICATION SETTINGS

Application settings which are general for all types of its tasks and regulating its operation in general, for example, application performance, logging, and Backup settings.

AVAILABLE UPDATE

A package of updates for the modules of a Kaspersky Lab application including a set of urgent patches released during a certain time interval, and modifications to the application architecture.

B

BACKUP FOLDER

Special folder for storage of Administration Server data copies created using the backup utility.

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 on computer security threats that are known to Kaspersky Lab by the moment 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

Managing the application 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.

G

GROUP TASK

A task defined for an administration group and performed on all client computers within this group.

I

INCOMPATIBLE APPLICATION

An anti-virus application from a third-party developer 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 on iOS platform managed by an iOS MDM mobile devices server (see section "iOS MDM mobile devices server" on page 84).

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

Kaspersky Lab servers to which the updated anti-virus database and the application modules are uploaded.

KASPERSKY SECURITY CENTER ADMINISTRATOR

The person managing the application operations through the Kaspersky Security Center system of remote centralized administration.

KASPERSKY SECURITY CENTER OPERATOR

A user who monitors the status and operation of a protection system managed with Kaspersky Security Center.

KASPERSKY SECURITY CENTER SYSTEM HEALTH VALIDATOR (SHV)

A component of Kaspersky Security Center application designed for checking the operating system's operability in case of concurrent operation of Kaspersky Security Center and Microsoft NAP.

KEY FILE

A file with the KEY extension that makes it possible to use a Kaspersky Lab application under a trial or commercial license. The application can be used only with a key file.

L

LICENSE TERM

License term is a time period during which you have access to the application features and 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.

M

MOBILE DEVICES SERVER

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

MOBILE DEVICES SERVER SUPPORTING EXCHANGE ACTIVESYNC

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

N

NETWORK AGENT

Network Agent is a component of Kaspersky Security Center that coordinates interaction between Administration Server and Kaspersky Lab applications installed on a specific network node (a workstation or a server). This component is common for all of the company's products for Windows. Special versions of Network Agent have been developed for Kaspersky Lab products for Novell, Unix, and Mac.

P

POLICY

A 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 defines 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 INSTALLATION

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 Sever (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 Kaspersky Lab's application are implemented as tasks, such as: Real-time file protection, Full computer scan, Database 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 replacement / addition of new files (databases or application modules), downloaded from the Kaspersky Lab's 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 is exceeded, it is interpreted as increased virus activity and as a threat of a virus attack. This property is important during periods of virus outbreaks since it enables administrators to react 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.

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 pocket computers, and 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), 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 official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com/
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending probably infected files in archive format)
	http://support.kaspersky.com/virlab/helpdesk.html
	(for queries addressed to virus analysts)
Kaspersky Lab web forum:	http://forum.kaspersky.com

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 respective owners.

Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Active Directory, ActiveSync, Internet Explorer, Microsoft, SQL Server, Windows, Windows Server and Windows Vista are registered trademarks of Microsoft Corporation in the United States and other countries.

Intel, Core and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Apple, iPhone, Mac and Mac OS are registered trademarks of Apple Inc.

Android is a trademark of Google, Inc.

Symbian trademark is owned by the Symbian Foundation Ltd.

Novell, Netware are either registered trademarks or trademarks of Novell, Inc. in the United States and/or other countries.

UNIX is a registered trademark in the United States and in other countries, used under license from X/Open Company Limited.

INDEX

L

M

N

P

R

S

T

U