Kaspersky Security Center 9.0

Implementation Guide

APPLICATION VERSION: 9.0 CRITICAL FIX 3

Dear User!

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

Kaspersky Lab reserves the right to amend this document without additional notification. The latest version of this document can be found on the Kaspersky Lab website, at http://www.kaspersky.com/docs.

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

Document revision date: 11/6/2013

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document describes installation of components of Kaspersky Security Center 9.0 (hereinafter referred to as Kaspersky Security Center) as well as remote installation of Kaspersky Lab applications on client computers.

This Guide is aimed at corporate network administrators responsible for anti-virus protection in organizations and SaaS providers (hereinafter referred to as *service providers*).

In cases actions of the service provider differ from those of the enterprise network administrator, actions of the service provider are described separately.

IN THIS SECTION:

IN THIS DOCUMENT

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

Additional sources of information (see page 8)

This section explains how to get information about the application apart from the documentation included in the distribution package.

Kaspersky Security Center (see page 10)

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

Application architecture (see page 11)

The section outlines the Kaspersky Security Center internal components and the logic of their cooperation.

Hardware and software requirements (see page 12)

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

Administration Server performance details (see page 14)

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

Typical schemes for deployment of anti-virus protection (see page 15)

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

Deploying anti-virus protection within an organization (see page 16)

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

Deploying anti-virus protection in a client organization's network (see page 18)

This section describes processes of anti-virus protection deployment on the network of a client enterprise that correspond to the standard deployment schemes.

Deploying Administration Server (see page 21)

This section describes stages of Administration Server deployment.

DOCUMENT CONVENTIONS

Document conventions described in the table below are used in this document.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and enclosed in frames. Notifications contain important information connected with critical actions related to computer security.
We recommend that you use...	Notes are framed in dotted-line boxes. Notes contain additional and reference information.
Example: ...	Example blocks have a yellow background, and the heading "Example".

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Update means...	New terms are italic.
ALT+F4	Names of keyboard keys are bold and are all uppercase. Names of the keys connected by a plus sign (+) indicate a combination of keys.
Enable	Names of interface elements are bold: for example, input fields, menu commands, and buttons.
➧ *To configure task schedule:*	Procedure headings are italic.
`help`	Text in the command line and text of messages displayed on the screen have a special font.
<Your computer's IP address>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value must be entered in each case; the angle brackets are omitted.

ADDITIONAL SOURCES OF INFORMATION

This section explains how to get information about the application apart from the documentation included in the distribution package.

If you have any questions regarding selection, purchase, installation or use of Kaspersky Security Center, you can quickly find relevant answers.

Kaspersky Lab provides various sources of information about the application. You can select the most suitable information source, depending on the issue's level of importance and urgency.

IN THIS SECTION:

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can view the following sources of information about the application:

- Application's page on Kaspersky Lab's website
- The application's page on the Technical Support Service's website (in the Knowledge Base)
- Help system
- Documentation

Application page on the Kaspersky Lab website

http://www.kaspersky.com/security-center

This page will provide you with general information about the application's features and options.

Application page on the Technical Support website (Knowledge Base)

http://support.kaspersky.com/remote_adm

This page contains articles by the Technical Support Service.

These articles contain useful information, recommendations, and answers to frequently asked questions (FAQ). The articles cover purchasing, installing, and using Kaspersky Security Center. The articles are grouped by subject, for example, "Working with key files", "Updating databases", or "Troubleshooting". The articles may contain answers to questions related not only to Kaspersky Security Center, but to other Kaspersky Lab products as well, and may contain general Technical Support Service news.

Online Help

The application installation package includes Full Help files.

They contain step-by-step descriptions of the application's features.

To open the Full Help file, select **Help Topics** in the console **Help** menu.

If you have a question about a specific application window, you can use context-sensitive Help.

To open context-sensitive Help, in the corresponding window press the **F1** key.

Documentation

The documentation supplied with the application aims to provide all the information you will require. It includes the following documents:

- **Administrator's Guide** – Describes the purpose, basic concepts, features, and general schemes for using Kaspersky Security Center.
- **Implementation Guide** – Contains a description of the installation procedures for the components of Kaspersky Security Center as well as remote installation of applications in computer networks that have a simple configuration.
- **Getting Started** – Gives step-by-step explanations that allow anti-virus security administrators to start using Kaspersky Security Center quickly, and to deploy Kaspersky Lab's anti-virus applications across a managed network.

The documents are included in .pdf format in the distribution package of Kaspersky Security Center.

You can download the documentation files from the application's page at the Kaspersky Lab website.

Information about the application programming interface (API) of Kaspersky Security Center is displayed in the klakaut.chm file, which is in the application installation folder.

DISCUSS KASPERSKY LAB APPLICATIONS AT THE ONLINE FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab experts and other users at our forum by visiting http://forum.kaspersky.com.

At this forum you can view existing discussion threads, leave comments, create new threads, and use search functionality.

CONTACTING THE TECHNICAL DOCUMENTATION DEVELOPMENT TEAM

If you have any questions about the documentation, or you have found an error in it, or would like to leave a comment, please contact our Documentation development group.

Click the **Leave feedback** link located in the top right part of the help window to open the computer's default mail client. The displayed window will automatically show the address of the Documentation Development Team (docfeedback@kaspersky.com) and the message subject "Kaspersky Help Feedback: Kaspersky Security Center". Write your comment and send your message without changing the subject line.

KASPERSKY SECURITY CENTER

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

The application is supplied in two versions:

- Kaspersky Security Center 9.0 (hereinafter also referred to as Kaspersky Security Center) is supplied for free with all Kaspersky Lab applications included in the Kaspersky Open Space Security (box version). You can also download it from the Kaspersky Lab website (http://www.kaspersky.com).
- Kaspersky Security Center 9.0, Service Provider Edition (hereinafter also referred to as Kaspersky Security Center SPE) is distributed under special conditions to Kaspersky Lab partners. For detailed information, please refer to Kaspersky Lab's website, the http://www.kaspersky.com/partners page.

The previous version of Kaspersky Security Center is Kaspersky Administration Kit.

Kaspersky Security Center is designed for centralized processing of the primary administrative tasks involved in managing a LAN anti-virus security system that is based on applications in the Kaspersky Open Space Security product family. Kaspersky Security Center supports interaction through all network configurations that use the TCP/IP protocol.

The Kaspersky Security Center application 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 provider*).

Using Kaspersky Security Center, you can:

- Create virtual Administration Servers to ensure the anti-virus protection of remote offices or networks of client organizations.

  The *client organization* is an organization, whose anti-virus protection is ensured by service provider.
- Create a hierarchy of administration groups to ensure anti-virus protection. Administration groups allow similar types of computers to be managed as a single unit.
- Remotely install and uninstall Kaspersky Lab applications.
- Centrally administer all installed Kaspersky Lab applications across the network, from a single computer.
- Centrally receive and distribute, on client computers, database updates and updates to application modules of Kaspersky Lab applications.
- Receive notifications about critical events in the operation of Kaspersky Lab applications.
- Receive statistics and reports about the operation of Kaspersky Lab applications.
- Manage keys for installed Kaspersky Lab applications.
- Centrally manage files put in Quarantine or Backup by anti-virus applications, and objects for which disinfection has been postponed.
- Centrally manage any third-party applications installed on the client computers.

APPLICATION ARCHITECTURE

The section outlines the Kaspersky Security Center internal components and the logic of their cooperation.

Kaspersky Security Center comprises the following main components:

- **Administration Server** (hereinafter also referred to as the *Server*). Centralizes the storage of information about Kaspersky Lab's applications installed in the corporate network and about their management.
- **Network Agent** (hereinafter also referred to as the *Agent*). Coordinates the interaction between Administration Server and Kaspersky Lab applications installed on a network node (workstation or server). This component is common to all applications included in Kaspersky Open Space Security products developed for Microsoft® Windows® systems. 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.
- **Kaspersky Security Center Web-Console**. Designed to manage the anti-virus protection status of client organization's networks that are protected 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

- Software requirements:
  - Microsoft Data Access® Components (MDAC) 2.8 or later, or 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 Express 2012, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, MySQL 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091 or MySQL Enterprise 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.
  - Microsoft Windows Server® 2003 or later; Microsoft Windows Server 2003 x64 or later; Microsoft Windows Server 2008; Microsoft Windows Server 2008, deployed in the Server Core mode; Microsoft Windows Server 2008 x64 with installed Service Pack 1 and all current updates (for Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 should be installed); Microsoft Windows Server 2008 R2; Microsoft Windows Server 2008 R2 deployed in the Server Core mode; Microsoft Windows Server 2012 (all editions); Microsoft Windows XP Professional with installed Service Pack 2 or later; Microsoft Windows XP Professional x64 or later; Microsoft Windows Vista® with installed Service Pack 1 or later, Microsoft Windows Vista x64 with installed Service Pack 1 and all current updates (for Microsoft Windows Vista x64 Microsoft Windows Installer 4.5 should be installed); Microsoft Windows 7; Microsoft Windows 7 x64; Microsoft Windows 8; Microsoft Windows 8 x64.
- Hardware requirements:
  - To work with a 32-bit Windows operating system you need:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 512 MB
    - 1 GB of available disk space
  - To work with a 64-bit Windows operating system you need:
    - Processor with operating frequency of 1.4 GHz or higher
    - RAM size – 512 MB
    - 1 GB of available disk space.

Administration Console

- Software requirements:
  - Microsoft Windows operating system.

    The supported version of the operating system is determined by the requirements for Administration Server.
  - Microsoft Management Console 2.0 or later.
  - Working with Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 or Microsoft Windows Vista requires installed Microsoft Internet Explorer® 7.0 or later.
  - Working with Microsoft Windows7 requires installed Microsoft Internet Explorer 8.0 or later.
  - Working with Microsoft Windows8 requires installed Microsoft Internet Explorer 10.0 or later.
- Hardware requirements:
  - To work with a 32-bit Windows operating system you need:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 512 MB

- 1 GB of available disk space
- To work with a 64-bit Windows operating system you need:
  - Processor with operating frequency of 1.4 GHz or higher
  - RAM size – 512 MB
  - 1 GB of available disk space.

Network Agent or Update Agent

- Software 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.
- Hardware requirements:
  - To work with a 32-bit Windows operating system you need:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 512 MB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
  - To work with a 64-bit Windows operating system you need:
    - Processor with operating frequency of 1.4 GHz or higher
    - RAM size – 512 MB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
  - To work with a 32-bit Linux operating system you need:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 1GB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
  - To work with a 64-bit Linux operating system you need:
    - Processor with operating frequency of 1.4 GHz or higher
    - RAM size – 1GB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent
  - To work with Mac OS operating system:
    - Processor with operating frequency of 1 GHz or higher
    - RAM size – 1GB
    - Available disk space: 32 MB for Network Agent, 500 MB for Update Agent.

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 2. 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 3. 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.

This document also presents detailed information about Administration Server performance testing.

TYPICAL SCHEMES FOR DEPLOYMENT OF ANTI-VIRUS PROTECTION

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

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

- Deploying anti-virus protection via Kaspersky Security Center, using one of the following methods:
  - by using the Administration Console
  - by using Kaspersky Security Center Web-Console.

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

  The basic deployment scheme is anti-virus protection deployment via the Administration Console. Using Kaspersky Security Center Web-Console allows starting installation of Kaspersky Lab applications from a browser.
- Deploying anti-virus protection manually using stand-alone 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 anti-virus protection using group policies of Active Directory®. For more details please refer to the Kaspersky Security Center Full Help.

DEPLOYING ANTI-VIRUS PROTECTION WITHIN AN ORGANIZATION

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

IN THIS SECTION:

DEPLOYING ANTI-VIRUS PROTECTION USING THE ADMINISTRATION CONSOLE WITHIN AN ENTERPRISE

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

1. The administrator deploys the Administration Server as follows:
   a. installs Kaspersky Security Center to a selected computer;
   b. installs the Administration Console on the administrator's workstation (if necessary);
   c. installs Kaspersky Security Center SHV to the administrator's workspace (if required);
   d. 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 the Network Agent and Kaspersky Lab anti-virus 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 carries out additional configuration of installed applications through the Administration Console using policies and local settings of applications.

DEPLOYING ANTI-VIRUS PROTECTION USING KASPERSKY SECURITY CENTER WEB-CONSOLE WITHIN AN ORGANIZATION

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

1. The administrator deploys the Administration Server as follows:
   a. installs Kaspersky Security Center to a selected computer;

   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator's workstation (if necessary);
   d. installs Kaspersky Security Center SHV to the administrator's workspace (if required);
   e. configure 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 the Network Agent and Kaspersky Lab anti-virus 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 carries out additional configuration of installed applications through the Administration Console using policies and local settings of applications.

DEPLOYING ANTI-VIRUS PROTECTION MANUALLY WITHIN AN ENTERPRISE

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

1. The administrator deploys the Administration Server as follows:
   a. installs Kaspersky Security Center to a selected computer;
   b. installs the Administration Console on the administrator's workstation (if necessary);
   c. installs Kaspersky Security Center SHV to the administrator's workspace (if required);
   d. 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 the Network Agent and Kaspersky Lab anti-virus 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 ANTI-VIRUS PROTECTION IN THE CLIENT ORGANIZATION NETWORK

This section describes processes of anti-virus protection deployment on the network of a client enterprise that correspond to the standard deployment schemes.

IN THIS SECTION:

DEPLOYING ANTI-VIRUS PROTECTION USING THE ADMINISTRATION CONSOLE ON THE NETWORK OF A CLIENT ENTERPRISE

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

1. The administrator of Kaspersky Security Center deploys Administration Server as follows:
   a. installs Kaspersky Security Center to a selected computer;
   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator's workstation (if necessary);
   d. installs Kaspersky Security Center SHV to the administrator's workspace (if required);
   e. configure Administration Server for work with Kaspersky Security Center Web-Console.
2. The administrator of Kaspersky Security Center creates a virtual Administration Server in Kaspersky Security Center to manage client computers in the client organization.
3. The administrator of Kaspersky Security Center selects a computer on the organization's network that should act as Update Agent, and installs Network Agent to it locally.

   As a result, Kaspersky Security Center automatically appoints the client computer on which the Network Agent is installed as the Update Agent and configures it as a connection gateway at the first connection to the Administration Server.
4. On the virtual Administration Server, the administrator of Kaspersky Security Center creates and configures installation packages of Network Agent and Kaspersky Lab anti-virus applications.
5. In Administration Console, the administrator of Kaspersky Security Center selects computers to which the selected applications should be installed.
6. The administrator creates and runs remote installation tasks for selected applications through the Administration Console.
7. If necessary, the administrator carries out additional configuration of installed applications through the Administration Console using policies and local settings of applications.

DEPLOYING ANTI-VIRUS PROTECTION USING KASPERSKY SECURITY CENTER WEB-CONSOLE IN A CLIENT ORGANIZATION'S NETWORK

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

1. The administrator of Kaspersky Security Center deploys Administration Server as follows:
   a. installs Kaspersky Security Center to a selected computer;
   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator's workstation (if necessary);
   d. installs Kaspersky Security Center SHV to the administrator's workspace (if required);
   e. configure Administration Server for work with Kaspersky Security Center Web-Console.
2. The administrator of Kaspersky Security Center creates a virtual Administration Server in Kaspersky Security Center to manage client computers in the client organization.
3. The administrator selects a computer on the network that should act as Update Agent, and installs the Network Agent on it locally.

   As a result, Kaspersky Security Center automatically appoints the client computer on which the Network Agent is installed as the Update Agent and configures it as a connection gateway at the first connection to the Administration Server.
4. On the virtual Administration Server, the administrator of Kaspersky Security Center creates and configures installation packages of Network Agent and Kaspersky Lab anti-virus applications.
5. In Kaspersky Security Center Web-Console the client enterprise administrator starts installation of selected applications on client computers.
6. If necessary, the administrator of Kaspersky Security Center performs additional configuration of installed applications via Administration Console using policies and local settings of applications.

DEPLOYING ANTI-VIRUS PROTECTION ON A CLIENT ENTERPRISE NETWORK MANUALLY

Manual installation of anti-virus 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 Administration Server as follows:
   a. installs Kaspersky Security Center to a selected computer;
   b. installs Kaspersky Security Center Web-Console to the same computer;
   c. installs the Administration Console on the administrator's workstation (if necessary);
   d. installs Kaspersky Security Center SHV to the administrator's workspace (if required);
   e. configure Administration Server for work with Kaspersky Security Center Web-Console.
2. The administrator of Kaspersky Security Center creates a virtual Administration Server in Kaspersky Security Center to manage client computers in the client organization.
3. The administrator selects a computer on the network that should act as Update Agent, and installs the Network Agent on it locally.

   As a result, Kaspersky Security Center automatically appoints the client computer on which the Network Agent is installed as the Update Agent and configures it as a connection gateway at the first connection to the Administration Server.

4. On the virtual Administration Server, the administrator of Kaspersky Security Center creates and configures installation packages of Network Agent and Kaspersky Lab anti-virus applications.
5. The administrator of Kaspersky Security Center creates standalone installation packages for selected applications.
6. Kaspersky Security Center administrator sends the standalone installation package to their client organization (for example, by publishing the link to the package in Kaspersky Security Center Web-Console).
7. The administrator of the client organization sends the standalone package to the selected computers through Kaspersky Security Center Web-Console.
8. Users of client computers start application installation by using a standalone installation package.
9. After the client computer is connected to Administration Server, it is moved to administration group specified the properties of the stand-alone package.

DEPLOYING ADMINISTRATION SERVER

This section describes stages of Administration Server deployment.

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

- Administration Server deployment within an organization;
- Administration Server deployment for anti-virus protection of a client organization (when using the SPE version of the application).

If you are required to deploy Administration Server within organization that includes the remote offices not included in the organization network, you can use the anti-virus protection deployment scenario for service providers.

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

STAGES OF ADMINISTRATION SERVER DEPLOYMENT FOR ANTI-VIRUS PROTECTION OF A CLIENT ENTERPRISE

To deploy the Administration Server for anti-virus protection of the client organization:

1. Install the Kaspersky Security Center on the administrator's workstation.
2. If required, install Kaspersky Security Center SHV on the administrator's workstation.
3. Install Kaspersky Security Center Web-Console on the administrator's workstation.
4. Configure Administration Server for cooperation with Kaspersky Security Center Web-Console.

UPGRADING THE PREVIOUS VERSION OF KASPERSKY SECURITY CENTER

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

To upgrade Administration Server of the 8.0 version to the 9.0 version:

1. Create a backup copy of the Administration Server data for Kaspersky Administration Kit 8.0 by using the *klbackup* utility. This utility is included in the application distribution, and is located in the root of the Kaspersky Administration Kit installation folder.

   Fully restoring Administration Server data from a backup copy requires storing the Administration Server certificate. The Administration Server certificate is required for the operation of the *klbackup* utility.

   For details about the operation of the data backup and recovery utility, see the *Kaspersky Security Center Administrator Guide*.

2. You can install Administration Server of the 9.0 version on a computer with a previous version of Administration Server. When you upgrade Administration Server to version 9.0, all data and settings from the previous version of the application are saved.

   Cancelling the product setup at an installation stage of Administration Server can cause Kaspersky Administration Kit 8.0 to fail.

3. For the selected computers, create and launch a remote deployment task for the new version of Network Agent. After successful task completion, Network Agent 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 KASPERSKY SECURITY CENTER

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

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

If at least one Administration Server is installed in the network, Servers can be installed to other computers remotely through the remote installation task using push installation (see section "Installing applications using a remote installation task" on page 40). When creating the remote installation task, you should use the Administration Server installation package.

IN THIS SECTION:

PREPARING TO INSTALLATION

Before starting the setup process, make sure that the hardware and software of the host computer meet the requirements for Administration Server and Administration Console (see section "Hardware and software requirements" on page 12).

Kaspersky Security Center stores its information in a SQL Server database. By default, for that purpose Microsoft SQL Server 2005 Express Edition is installed together with Kaspersky Security Center. Other SQL Servers can also be used for data storage (see section "Hardware and software requirements" on page 12). 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 4. Ports used by Kaspersky Security Center

PORT NUMBER	PROTOCOL	DESCRIPTION
Computer on which the Administration Server is installed		
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.
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.
13000	UDP	Used to transfer information if a computer is shut down.
13292	TCP	The port is used for connection of mobile devices.
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		
15,000	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.
7	UDP	The port is used by the Wake On LAN feature.

For outbound connections of client computers to the Administration Server and Update Agents, the range of ports 1024–5000 (TCP) is used. In Microsoft Windows Vista and Microsoft Windows Server2008 the default range of ports for outbound connections is 49152–65535 (TCP).

STANDARD INSTALLATION

To perform 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 carefully. If you accept the listed 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 2005 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.

THE WIZARD'S STEPS

STEP 1. VIEWING THE LICENSE AGREEMENT

At this stage of the Setup Wizard, read the License Agreement between you and Kaspersky Lab.

Read the License Agreement carefully. If you accept the listed 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, cancel the installation by clicking the **Close** button.

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

STEP 2. SELECTING INSTALLATION METHOD

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 a size of the network in which Kaspersky Security Center is to be 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 5. 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.

  A proper functioning of Kaspersky Security Center requires that the account used to start Administration Server has the administrator rights on 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 more details please 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 5,000 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 SQL Server is not installed in the network, select the option **Install Microsoft SQL Server 2005 Express Edition**.

    The Setup Wizard will then install Microsoft SQL Server 2005 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 12).

If you are installing the server on a remote computer, there is no need to interrupt the Kaspersky Security Center Setup Wizard. Install SQL Server and return to the 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 KLSHARE subfolder in the program folder containing the components of Kaspersky Security Center.

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 properties of the Kaspersky Lab Posture Validation Server (PVS) for Cisco NAC, This service will be running on the computer if the Kaspersky Lab policy server for Cisco NAC has been installed together with the Administration Server.

Table 6. Service attributes

PROPERTY	ADMINISTRATION SERVER	KASPERSKY LAB CISCO NAC POSTURE VALIDATION SERVER	NETWORK AGENT
Service name	kladminserver	klnacserver	klnagent
Displayed service name	Kaspersky Security Center Administration Server	Kaspersky Lab Cisco NAC Posture Validation Server	Kaspersky Security Center Network Agent
Startup type	Automatically when the operating system starts up		
Account	User-defined or dedicated account in KL-AK-* format created during the installation	*Local system*	

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.

REMOVING THE APPLICATION

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

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

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

INSTALLING ADMINISTRATION CONSOLE ON THE ADMINISTRATOR'S WORKSTATION

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

To install Administration Console on the administrator's workstation:

1. Run the setup.exe file from the CD containing the distribution package of Kaspersky Security Center in the Console folder.

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

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

2. Select a destination folder. By default, this will be <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.
3. In the last window of the Setup Wizard click the **Start** button to start the Administration Console installation.

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

After installing Administration Console, you must connect to the Administration Server. Start Administration Console. In the window that opens, specify the name of the computer on which Administration Server is installed and the settings of the account used to connect to it. After connection to Administration Server is established, you can manage the anti-virus protection system using this Administration Console.

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

INSTALLING AND CONFIGURING KASPERSKY SECURITY CENTER SHV

Kaspersky Security Center supports integration with the Microsoft Network Access Protection (NAP). Microsoft NAP allows regulation of client computer access to the network. Microsoft NAP assumes that the network includes a dedicated server with Microsoft Windows Server2008 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 (referred to as Kaspersky Security Center SHV).

To install Kaspersky Security Center SHV to a computer locally:

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

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

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

2. Specify the destination folder. By default, this will be <Drive>:\Program Files\Kaspersky Lab\Kaspersky Security Center SHV. If such folder does not exist, it is created automatically during the installation. You can change the destination folder by using the **Browse** button.
3. In the last window of the Setup Wizard click the **Start** button to start the installation of Kaspersky Security Center SHV.

After the wizard completes, Kaspersky Security Center SHV will be installed on your computer.

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

INSTALLING KASPERSKY SECURITY CENTER WEB-CONSOLE

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

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

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

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

THE WIZARD'S STEPS

STEP 1. VIEWING THE LICENSE AGREEMENT

At this stage of the Setup Wizard, read the License Agreement between you and Kaspersky Lab.

Read the License Agreement carefully. If you accept the listed 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, cancel the installation by clicking the **Close** button.

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

STEP 2. SELECTING THE DESTINATION FOLDER

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

STEP 3. SELECTING THE PORTS

Specify the following settings:

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

STEP 4. CONNECTING TO KASPERSKY SECURITY CENTER

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

- **Use Apache server installed on local computer**. If this option is selected, Kaspersky Security Center Web-Console will be connected to Kaspersky Security Center via the Apache server installed on a local computer (you can select installation of Apache server at the next step of the Wizard).
- **Use Apache server installed on remote computer**. You can select this option if the Apache server is already installed on a remote computer running under Linux. In this case, only the server part of Kaspersky Security Center Web-Console will be installed. To connect Kaspersky Security Center Web-Console to Kaspersky Security Center, you should install the client part of Kaspersky Security Center Web-Console to a remote computer. If you select this option, the Setup Wizard proceeds to Step 7 (see section "Step 7. Starting installation of Kaspersky Security Center Web-Console" on page 33).

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 following methods:
  - **Select certificate file** You can select an existing certificate by clicking the **Browse** button.
  - **Select a private key**. You can specify a certificate using the file of its closed key by clicking the **Browse** button.

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

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

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

The installation process is displayed on the Wizard page.

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

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

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

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

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

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

   Configure the virtual server settings as follows:

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

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

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

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

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

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

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

1. Prepare a logo file meeting the following requirements:
   - File format: PNG

- File name: logo.png
- File size: any
- 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 Administration Server's cooperation with Kaspersky Security Center Web-Console please refer to the *Kaspersky Security Center Administrator's Guide*.

CONFIGURING ANTI-VIRUS PROTECTION SYSTEM IN THE NETWORK OF A CLIENT ORGANIZATION

This section describes features typical of setup of an anti-virus protection system using Administration Console on the network of a client enterprise.

Configuring anti-virus protection system makes part of the process of anti-virus protection deployment on the network of a client enterprise. The procedure of anti-virus 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 the Network Agent and Kaspersky Lab anti-virus applications to computers of the client enterprise.

   This section describes prerequisites for remote installation of applications to computers of a client enterprise. The procedure of remote installation of Network Agent and Kaspersky Lab anti-virus applications is described in details in the Remote installation of applications section (see page 39).

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:

REQUIREMENTS TO INSTALLATION OF APPLICATIONS ON COMPUTERS OF A CLIENT ENTERPRISE

Remote installation of applications to computers of a client organization is identical to that within an enterprise (see section "Remote installation of software" (see page 39)).

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 given in the *Kaspersky Security Center Administrator's Guide*.

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

REMOTE INSTALLATION OF APPLICATIONS

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

Before you start installation of applications to client computers, make sure that the hardware and software on target computers meet the system requirements (see section "Hardware and software requirements" on page 12).

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). However, remote management through Kaspersky Security Center will be available for those applications.

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

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

If remote installation of an application completes with an error, you can find the cause of this error and fix it using the remote deployment preparation utility (see section "Preparing computer for remote installation.). Utility tool riprep.exe" on page 47).

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 8 for Smartphone
- Kaspersky Endpoint Security 8 for Mac

- Kaspersky Endpoint Security 8 for Linux
- Kaspersky Security for Virtualization 1.1.

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 open automatically using the Deployment preparation utility (see section "Preparing computer for remote installation. Utility tool riprep.exe" on page 47).

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

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

To install an application using Active Directory group policies:

1. Run the creation of group remote installation task or remote installation task for specific computers.
2. In the New Task Wizard's **Settings** window select the **Assign the package installation in the Active Directory group policies** check box.
3. Run the created remote installation task manually or wait for its scheduled start.

This starts the following remote installation sequence:

1. After the task is started, the following objects are created in each domain that includes the client computers from the specified set:
   - A group policy under the name **Kaspersky_AK{GUID}**
   - the **Kaspersky_AK{GUID}** security group that corresponds to the group policy. This security group includes client computers covered by the task. The content of the security group defines the scope of the group policy.
2. In this case, applications are installed on client computers directly from the Kaspersky Security Center shared network folder **KLSHARE**. In the Kaspersky Security Center installation folder, an auxiliary nested folder will be created that contains the .msi file for the application to be installed.

3. When new computers are added to the task scope, they are added to the security group after the next task start. If the **Run missed tasks** check box is selected in the task schedule, computers are added to the security group immediately.
4. When computers are deleted from the task scope, they are deleted from the security group after the next task start.
5. When a task is deleted from Active Directory, the policy, the link to the policy, and the corresponding security group are deleted.

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

- when the anti-virus protection administrator does not have rights to make changes to the Active Directory of certain domains;
- when the original installation package needs to be stored on a separate network resource;
- when it is necessary to link a group policy to specific Active Directory units.

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

- If installation is to be performed directly from the Kaspersky Security Center shared folder, in the Active Directory group policy properties you must specify the .msi file located in the exec subfolder of the installation package folder for the required application.
- If the installation package has to be located on another network resource, you must copy the whole exec folder content to it, because in addition to the file with .msi extension the folder contains configuration files generated when the package was created. To install the key with the application, copy the key file to this folder as well.

INSTALLING APPLICATIONS ON SLAVE ADMINISTRATION SERVERS

To install an application on slave Administration Servers:

1. Establish a connection with the Administration Server that controls the relevant slave Administration Servers.
2. Make sure that the installation package corresponding to the application being installed is available on each one of the selected slave Administration Servers. If the installation package cannot be found on any of the slave Servers, distribute it by using the installation package distribution task (see see section "Distributing installation packages to slave Administration Servers" on page 45).
3. Start the creation of the task of application installation on slave Administration Servers in one of the following ways:
   - If you want to create a task for the slave Servers of a selected administration group, run creation of a group task of remote installation for that group (see section "Installing the application to client computers in an administration group" on page 41).
   - If you want to create a task for selected slave Servers, run creation of a remote installation task for specific computers (see section "Installing the application to selected client computers" on page 40).

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

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

   The New Task Wizard will create the task of remote deployment of the selected application on specific slave Administration Servers.
4. Run the task manually or wait for it to launch according to the schedule specified by you in the task settings.

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

INSTALLING APPLICATIONS USING REMOTE INSTALLATION WIZARD

To install Kaspersky Lab applications, you can use the Remote Installation Wizard. The Remote Installation Wizard allows remote deployment of applications with specially created installation packages or directly from a distribution package.

For correct remote installation on the client computer on which Network Agent has not been installed, the following ports must be opened: TCP 139 and 445; UDP 137 and 138. By default, these ports are open for all computers included in the domain. They are opened automatically by using the Deployment preparation utility (see section "Preparing computer for remote installation. Utility tool riprep" on page 47)

To install the application using the Remote Installation Wizard:

1. Establish a connection with the Administration Server that controls the relevant administration group.
2. Select an administration group in the console tree.
3. In the group workspace, open the **Groups** tab.
4. Launch application installation by clicking the **Start installation** link in the **Remote installation** section.

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

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

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

- Creates an installation package for application installation (if it was not created earlier). The installation package is located in the **Storages** folder inside the **Installation packages** subfolder and has a name corresponding to the application name and version. You can use this installation package for the application installation in the future.
- Creates and starts a remote installation task for specific computers or for an administration group. The created remote deployment task is stored in the **Tasks for specific computers** folder or is added to the tasks of the administration group for which it has been created. You can later launch this task manually. The task name corresponds to the name of the application installation package: **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 UNINSTALLATION OF APPLICATIONS

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

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

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

IN THIS SECTION:

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

To remove an application remotely from client computers of the administration group:

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

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

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

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

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

REMOTE REMOVAL OF AN APPLICATION FROM SPECIFIC CLIENT COMPUTERS

To remove an application remotely from specific client computers:

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

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

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

   The New Task Wizard creates a task of remote removal of the selected application from specific computers. The new 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 a single installation package several times.

Installation packages created for an Administration Server are located in the **Repositories** folder, the **Installation packages** subfolder of the console tree. 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 console tree, select the **Repositories** folder, 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, to re-create it you select the nagent9.kud file in the NetAgent folder of the Kaspersky Security Center distribution package.

When an installation package for Administration Server is created, 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 New Task Wizard, in the **Kaspersky Security Center Administration Server** node, open the **Advanced** folder and select the task type named **Distribute installation package**.

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

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

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

DISTRIBUTING INSTALLATION PACKAGES BY USING UPDATE AGENTS

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

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

TRANSFERRING APPLICATION INSTALLATION RESULTS TO KASPERSKY SECURITY CENTER

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

1. Navigate to the folder of the installation package created by using Kaspersky Security Center for the selected application. The folder can be found in the shared folder specified during Kaspersky Security Center installation.
2. Open the file with the .kpd or .kud extension for editing (for example, in the Microsoft Windows Notepad editor). The file has the format of a regular configuration .ini file.
3. Add the following lines to the file:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   This command configures Kaspersky Security Center to wait for setup completion for the application, for which the installation package is created, and to analyze the installer return code. If you have to disable the transfer of diagnostic data, set the Wait key to 0.
4. Add the description of return codes for a successful installation. To do this, add the following lines to the file:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   …
   ```

   Square brackets contain optional keys.

   Syntax for the lines:

   - `<return code>`. Any number corresponding to the installer return code. The number of return codes can be arbitrary.
   - `<description>`. Text description of the installation result. The description can be omitted.
5. Add the description of return codes for a failed installation. To do this, add the following lines to the file:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   …
   ```

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

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

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

RETRIEVING UP-TO-DATE VERSIONS OF APPLICATIONS

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

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

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

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

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

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

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

- The task has already been successfully performed on this computer. In this case, the task does not have to be performed again.
- When a task was started, the computer was off. In this case turn on the computer and restart the task.

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

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

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

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

IN THIS SECTION:

PREPARING THE COMPUTER FOR REMOTE DEPLOYMENT IN INTERACTIVE MODE

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 Data Protection Suite
- 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 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 36).

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 NON-INTERACTIVE MODE

To install an application in non-interactive mode:

1. Open the main window of Kaspersky Security Center.
2. In the **Storages** folder of the console tree, open the **Installation packages** subfolder and select the installation package of the requisite application or create a new installation package for this 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 of the requisite 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 selected application, do the following:
   - For Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers and Kaspersky Security Center, navigate to the exec subfolder and run the executable file (the one with the .exe extension) with the /s key.
   - for other Kaspersky Lab applications run the executable file (a file with the .exe extension) with the /s key from the open folder.

INSTALLING SOFTWARE BY USING STAND-ALONE PACKAGES

Kaspersky Security Center allows creating standalone installation packages for applications. A standalone installation package is an executable file that can be located on the web server, sent by email, or transferred to a client computer in any other way. The received file can be run locally on the computer to install an application without involving Kaspersky Security Center.

To install an application using a standalone installation package:

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

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

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

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

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

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 9.0 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 7. 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 8. 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 9. 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 10. 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 N stands 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 N stands for the total number of computers included in the administration group.

PROCESSING OF EVENTS FROM CLIENTS BY ADMINISTRATION SERVER

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

Table 11. 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 12. 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 Server was 20 minutes, updates were downloaded to the Administration Server storage once per hour.

RATE OF ADDING KASPERSKY ENDPOINT SECURITY EVENTS TO THE DATABASE

This section contains examples of filling the Administration Server database with events.

(Ne*Nh) events per day are added to the database (see table below). Here Nh is the number of client computers where Kaspersky Endpoint Security is installed, Ne is the number of events per day that are informed of by Kaspersky Endpoint Security installed on a client computer.

Table 13. Rate of database filling with events

NUMBER OF COMPUTERS WITH KASPERSKY ENDPOINT SECURITY INSTALLED	NUMBER OF EVENTS ADDED TO THE DATABASE PER DAY
100	≤ 2 000
1000	≤ 20 000
10,000	≤ 200 000

The table contains data for standard run mode of Kaspersky Endpoint Security allowing not more than 20 events per day to be received from each client computer.

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

CONTACTING TECHNICAL SUPPORT SERVICE

You can obtain information about the application from the Technical Support Service, by phone or on the Internet. When contacting the Technical Support Service, you will need to provide information about the license for Kaspersky Security Center.

Technical Support Service will answer any questions related to the installation and use of the application that are not covered in Help topics. If your computer has been infected, they will help you to neutralize the consequences of malware activity.

Before contacting the Technical Support Service, please read the support rules for Kaspersky Lab products http://support.kaspersky.com/support/rules.

Technical Support by email

You can send your question to Technical Support Service by filling out a Helpdesk web form for client questions at http://support.kaspersky.com/helpdesk.html.

You can send your inquiry in Russian, English, German, French or Spanish.

To send an email request, you should specify your **customer ID**, which you received while registering at the Technical Support Service's website, and the corresponding **password**.

If you are not yet a registered user of Kaspersky Lab applications, you can fill out a registration form (https://support.kaspersky.com/en/personalcabinet/registration/form/). During registration you will need to enter either your application's *activation code*, or indicate the *key file*.

The Technical Support service will reply to your request in your Personal Cabinet (https://support.kaspersky.com/en/PersonalCabinet) and to the email address you have specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. In the mandatory fields, specify:

- **Request type**. Questions that users often ask are split into separate topics, for example: "Problems with Setup / Remove application" or "Virus disinfection". If you do not find an appropriate topic, select "General question".
- **Application name and version number**.
- **Request description**. Describe the problem you encountered in as much detail as possible.
- **Customer ID and password**. Enter the client number and the password you received when you registered at the Technical Support Service's website.
- **Email address**. The Technical Support service will send their answer to this email address.

Technical support by phone

If you have an urgent problem, you can call your local Technical Support Service. Before contacting Technical Support, please have the necessary information (http://support.kaspersky.com/support/details) about your computer handy. This will let our specialists help you more quickly.

GLOSSARY

A

Active key

Key that is used at the moment to work with the application.

Additional key

Key that verifies the use of 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 Server

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

Administration Server certificate

The certificate used for the Administration Server authentication during connection of Administration Consoles to it and data exchange with client computers. The Administration Server certificate is created and installed on Administration Server in the ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder.

Administration Server client (Client computer)

A computer, server, or workstation on which Network Agent and managed Kaspersky Lab applications are running.

Administration Server data backup

Copying of the Administration Server data for backup and subsequent restoration performed by using the backup utility. The utility can save:

- Information database of the Administration 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

Administration group

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

Administrator's workstation

Computer with an installed component that provides an application management interface. For anti-virus products, this component is Anti-Virus Console, and for Kaspersky Security Center it is Administration Console.

The administrator's workstation is used to configure and manage the server portion of the application. For Kaspersky Security Center it is used to build and manage a centralized anti-virus protection system for a corporate LAN based on Kaspersky Lab applications.

Application management plug-in

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

APPLICATION SETTINGS

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.

D

DATABASES

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

DIRECT APPLICATION MANAGEMENT

Application management through a local interface.

E

EVENT SEVERITY

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

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

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

G

GROUP TASK

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

I

INCOMPATIBLE APPLICATION

Anti-virus application of another vendor or a Kaspersky Lab application that does not support management through Kaspersky Security Center.

INSTALLATION PACKAGE

A set of files created for remote installation of a Kaspersky Lab application by using the Kaspersky Security Center remote administration system. An installation package is created based on special files with the .kpd and .kud extensions that are included in the application distribution package; it contains a set of settings required for application setup and its configuration for normal functioning immediately after installation. Parameter values correspond to application defaults.

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.

KEY FILE

A file with the .key extension that makes it possible to use a Kaspersky Lab application on the terms of a trial or commercial license. The application creates a key file based on the activation code. The application can be used only with a key file.

L

LICENSE VALIDITY PERIOD

License term is a time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

LOCAL TASK

A task defined and running on a single client computer.

LOGON SCRIPT-BASED INSTALLATION

Method for remote installation of Kaspersky Lab applications that allows you to link the start of a remote setup task to specified user account or accounts. When the user logs in to the domain, the system attempts to install the application on the corresponding client computer. This method is recommended for remote installation of the company's applications to computers running Microsoft Windows 98 / Me operating systems.

N

NETWORK AGENT

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

P

POLICY

A 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.

PROTECTION STATUS

Current protection status, which reflects the level of computer security.

PUSH INSTALLATION

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

R

REMOTE INSTALL

Installation of Kaspersky Lab applications by using the services provided by Kaspersky Security Center.

RESTORATION OF ADMINISTRATION SERVER DATA

Restoration of Administration Server data from the information saved in Backup by using the backup utility. The utility can restore:

- Information database of the Administration 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 replacing / adding new files (databases or application modules), received from the Kaspersky Lab update servers.

UPDATE AGENT

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

V

VIRUS ACTIVITY THRESHOLD

Maximum allowed number of events of the specified type within a limited time; when this number is exceeded, it is interpreted as increased virus activity and as a threat of a virus attack. This feature is important during periods of virus outbreaks because it enables administrators to respond in a timely manner to virus attack threats.

KASPERSKY LAB ZAO

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

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

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

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

The personal product range includes anti-virus applications for desktop, laptop, and 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's website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending probably infected files in archive format) http://support.kaspersky.com/helpdesk.html (for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

TRADEMARK NOTICE

The registered trademarks and service marks are the property of their 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, Data Access, 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.

Mac and Mac OS are registered trademarks of Apple Inc.

Novell is a registered trademark of Novell, Inc in the United States and other countries.

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

INDEX

U