

KASPERSKY LAB

Kaspersky[®] Administration Kit 6.0

Deployment Guide

KASPERSKY® ADMINISTRATION KIT 6.0

Deployment Guide

Kaspersky Lab Ltd.

Visit our website: <http://www.kaspersky.com/>

Revision date: February 2007.

Contents

CHAPTER 1. KASPERSKY® ADMINISTRATION KIT	5
1.1. Purpose, structure and main functions	5
1.2. Software and Hardware Requirements	7
1.3. Distribution kit	9
1.4. Help desk for registered users	9
1.5. The purpose of this document	9
1.6. Conventions.....	10
CHAPTER 2. TYPICAL SCHEMES OF DEPLOYMENT OF ANTI-VIRUS PROTECTION.....	11
2.1. Schemes of deployment of anti-virus protection on the computers within the logical network	11
2.2. Building a centralized anti-virus protection administration system	12
CHAPTER 3. INSTALLING KASPERSKY ADMINISTRATION KIT	14
3.1. Installing MSDE from the Kaspersky Administration Kit distribution package ..	16
3.2. Installing the Administration Server and Administration Console on Local Host	18
3.3. Removing Kaspersky Administration Kit components	34
3.4. Updating the application version.....	34
CHAPTER 4. INSTALLATION AND REMOVAL OF SOFTWARE ON THE COMPUTERS	36
4.1. Remote software installation	37
4.1.1. Creating an installation package	38
4.1.2. Reviewing and configuring the installation package settings.....	41
4.1.3. Creating and configuring the Network Agent installation package	46
4.1.4. Creating and Configuring Administration Server Installation Package	50
4.1.5. Creating a task for distribution of the installation package on the slave Administration Servers.....	50
4.1.6. Distribution of the installation packages within a group using network agents.....	52

4.1.7. Configuring the deployment task.....	67
4.1.8. Deploying application to slave administration servers.....	69
4.1.9. Remote software removal	71
4.2. Deployment wizard.....	72
4.3. Local software installation	76
4.3.1. Local installation of the Network Agent.....	77
4.3.2. Local installation of the application administration plugin.....	82
4.3.3. Installing applications in non-interactive mode	83
APPENDIX A. GLOSSARY	85
APPENDIX B. KASPERSKY LAB.....	92
B.1. Other Kaspersky Lab Products	93
B.2. Contact Us.....	103
APPENDIX C. LICENSE AGREEMENT	104

CHAPTER 1. KASPERSKY® ADMINISTRATION KIT

1.1. Purpose, structure and main functions

Kaspersky® Administration Kit is an application that is designed to provide a centralized solution for most important administration tasks associated with managing the corporate network anti-virus security system based on Kaspersky Lab's applications included into Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite. Kaspersky Administration Kit supports all network configurations that use TCP/IP protocol.

Kaspersky Administration Kit is a tool for corporate network administrators and anti-virus security officers.

The application enables the administrator to:

- Deploy or remove Kaspersky Lab applications across a network connection to computers within the network. This feature enables the administrator to copy the required set of Kaspersky Lab's applications to a selected computer and then deploy these applications on the network computers.
- Ensure remote centralized management of Kaspersky Lab applications. This feature enables the administrator to create a multi-level anti-virus protection system and manage the operation of all applications from a single administrator's workstation. This is particularly important for larger companies that have a local network consisting of a large number of computers that may cover several separate buildings or offices. This feature enables the administrator to:
 - group computers into *administration groups* based on the functions performed by such computers and the set of applications installed on them;
 - configure the application settings in a centralized way by creating and applying group policies;
 - configure individual settings of the application for individual computers using the application settings.
 - manage the operation of the applications in a centralized way by creating and running *group and global tasks*.

- create individual patterns for the application's operation by creating and running tasks for a set of computers from different administration groups.
- Automatically update the anti-virus database and application modules on computers. This feature allows centralized updating of the anti-virus database for all installed Kaspersky Lab's applications without accessing the Kaspersky Lab's internet updates server for each individual update. The updating can be performed automatically according to the schedule set up by the administrator. The administrator can monitor the installation of the updates on the client computers.
- Receive reports using a dedicated system. This feature allows centralized collection of statistical information about the operation of all installed Kaspersky Lab's applications, monitoring the correctness of the operation of these applications and creating reports based on the information obtained. The administrator can create a cumulative network report about the operation of an application or reports about the operation of application installed on each computer.
- Use events notification system. Mail notification sending system. This feature allows the administrator to create a list of events in the operation of the applications about which he or she will receive notifications. The list of such event may, for example, include detection of a new virus or an error that occurred when attempting to update the anti-virus database on a computer, detection of a new computer in the network.
- Perform license management. This capability supports centralized installation of license keys for all installed enterprise applications, tracking of compliance with the license agreement (number of licenses should correspond to number of running applications) and license agreement expiration date.
- Cooperate with Cisco Network Admission Control (NAC). This functionality provides a mapping between host antivirus protection conditions and Cisco NAC statuses.

Kaspersky Administration Kit application consists of three main components:

- **Administration server** performs the function of centralized storage of information about Kaspersky Lab's applications installed in the corporate network and about managing such applications.
- **Network Agent** coordinates the interaction between the Administration Server and Kaspersky Lab's applications installed on a specific network node (a workstation or a server). This component supports all Windows-applications included in the Kaspersky Lab Business Optimal and

Kaspersky Corporate Suites. Separate versions of Administration Agent exist for Kaspersky Lab Novell and UNIX applications.

- **Administration Console** provides a user interface to the administration services of the Administration Server and Network Agent. The management module is implemented as the extension of the Microsoft Management Console (MMC).

1.2. Software and Hardware Requirements

Administration Server

- Software requirements
 - Microsoft Data Access Components (MDAC) version 2.8 and above
 - MSDE 2000 SP 3 or MS SQL Server 2000 SP 31 or higher or MySQL version 5.0.22 (default code page UTF-8) or MS SQL 2-5 or higher or MS SQL 2005 Express or higher;
 - Microsoft Windows 2000 SP 1 or higher; Microsoft Windows XP Professional SP 1 or higher; Microsoft Windows XP Professional x64 and higher, Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003x64 or higher Microsoft Windows NT4 SP 6a or higher, Microsoft Windows Vista, Microsoft Windows Vista x64..
- Hardware requirements:
 - Intel Pentium III processor, 800 MHz or faster
 - 128 MB RAM
 - 400 MB available space on hard drive

Administration Console

¹ You can install MSDE from the package included in the Kaspersky Administration Kit distribution package.

- Software requirements:
 - Microsoft Windows 2000 SP 1 or higher; Microsoft Windows XP Professional SP 1 or higher; Microsoft Windows XP Professional x64 and higher, Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003x64 or higher Microsoft Windows NT4 SP 6a or higher, Microsoft Windows Vista, Microsoft Windows Vista x64;
 - Microsoft Management Console version 1.2 or higher
 - When running under Microsoft Windows NT4 you need Microsoft Internet Explorer 6.0 installed.
- Hardware requirements:
 - Intel Pentium II processor, 400 MHz or faster
 - At least 64 MB RAM
 - 10 MB of available hard drive space

Network Agent

- Software requirements:
 - For Windows systems:
 - Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 SP 1 or higher; Microsoft Windows NT4 SP 6a or higher; Microsoft Windows XP Professional x64 or higher, Microsoft Windows XP Professional SP 1 or higher, and Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher, Microsoft Windows Vista, Microsoft Windows Vista x64;
 - For Novell systems:
 - Novell NetWare 6 SP or higher; Novell NetWare 6.5 SP3 or higher
- Hardware requirements:
 - For Windows systems:
 - Intel Pentium processor, 233 MHz or faster
 - 32 MB RAM
 - 10 MB available space on hard drive
 - For Novell systems:
 - Intel Pentium processor, 233 MHz or better
 - 12 MB RAM

- 32 MB free (available) space on hard drive

1.3. Distribution kit

This software product is supplied free-of-charge with any Kaspersky Lab's application included into the package of Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite (retail box version) and also available for download from Kaspersky Lab's corporate website at www.kaspersky.com.

1.4. Help desk for registered users

Kaspersky Lab offers a large service package, enabling its legal users to enjoy all available features of Kaspersky Lab's products.

Once you purchase a license for any Kaspersky Lab's product included into Kaspersky Anti-Virus Business Optimal or Kaspersky Corporate Suite, you become a registered user of Kaspersky Administration Kit. After this you will receive the following services during the term of your license:

- New versions of the anti-virus software application;
- Consultations on matters related to the installation, configuration, and operation of the anti-virus application by phone or based on requests sent using a web form;

When sending a request to the Technical support service, make sure you specify information about the license for Kaspersky Lab's application used in conjunction with Kaspersky Administration Kit.

- Information about new Kaspersky Lab applications and about new computer viruses (for those who subscribe to the Kaspersky Lab newsletter).

Kaspersky Lab does not provide information related to operation and use of your operating system or various other technologies.

1.5. The purpose of this document

This Guide contains a description of the installation of Kaspersky Administration Kit and remote installation of applications within a computer network of simple configuration.

General concepts and application operation scheme are provided in the Kaspersky Administration Kit Administrator's Guide; step-by-step description of

actions when using the application is provided in the Kaspersky Administration Kit Reference Book.

In order to review questions that our users often ask Kaspersky Lab's support specialists visit our website and follow the **Services** → **Knowledge base** link. This section contains information about installation, configuration and functioning of Kaspersky Lab's applications and about removal of most commonly spread viruses and disinfection of infected files.

1.6. Conventions

Various formatting features and icons are used throughout this document depending on the purpose and the meaning of the text. The table below lists the conventions used in the text.

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.
Note	Additional information, notes.
Attention	Information you should pay special attention to.
<i>To perform an action:</i> <ol style="list-style-type: none"> 1. Step 1. 2. ... 	Description of the successive user's steps and possible actions
[modifier] – modifier name.	Command line modifier
Information messages and command line text	Text of configuration files, information messages and command line

CHAPTER 2. TYPICAL SCHEMES OF DEPLOYMENT OF ANTI-VIRUS PROTECTION

2.1. Schemes of deployment of anti-virus protection on the computers within the logical network

There are two common scenarios that show how you can deploy reliable anti-virus protection using Kaspersky Administration Kit:

- You can remotely install applications on client computers across the logical network from a single workstation. The installation and connection to the remote management system proceed automatically, requiring no interaction from the administrator and allowing to install the anti-virus software on any number of client computers.
- You can locally install applications on every networked computer. In this case, all required components and the administrator workstation are manually installed. Connection settings are set during the installation of the Network Agent. This deployment scenario is used only if centralized deployment is impossible.

Remote installation can be used for installation of any applications selected by the user.

However, bear in mind that Kaspersky Administration Kit supports administration of only Kaspersky Lab's application the distribution package of which includes a specialized component - the application administration plugin.

2.2. Building a centralized anti-virus protection administration system

The first step to building a system of centralized management over an enterprise network through Kaspersky Administration Kit is to design a logical network. At this stage, you should make the following decisions:

1. Select isolated sections within the network and determine the number of Administration servers that must be installed. The use of hierarchy of administration servers will allow to considerably decrease the load on the communication channels and increase the system reliability.
2. Which computers in the corporate network structure will function as the main Administration server, the slave servers administrator servers, administrator's workstations, and client computers. Note that all computers on which Kaspersky Lab applications are installed will act as client computers.
3. Which criteria will be used to organize client computers in groups? What will be the group hierarchy?
4. Which deployment scenario will be used: remote or local installation?

During the next stage, the administrator has to build a logical network, i.e., install the following Kaspersky Administration Kit components on networked computers, namely:

1. Install the Administration Servers on computers within the corporate network.
2. Install the Administration Console on computers from which the administration will be provided.
3. Make decision regarding assigning of the logical network administrators, determine which other user categories will interact with the system and assign a list of functions to be performed to each category.
4. Create lists of users and grant to each group access rights required to perform functions assigned to this group and related to access rights.

After this, it is required to create a hierarchy of the Administration servers and for each Server create a logical network structure as follows: create a hierarchy of the administration groups and distribute computers among the corresponding groups.

During the next stage, you should install the Network Agent and selected Kaspersky Lab applications on client computers and install the corresponding administration plugins on the administrator workstation.

If you use the remote installation option, the Network agent may be installed together with any application, in this case no separate installation of the Network agent is required.

During the final step, you should configure the installed applications by assigning and applying group policies and creating tasks.

Using the Quick Start Wizard, the administrator can easily build an anti-virus protection system for his/her network and perform minimum configuration. Briefly configuring the anti-virus protection system means creating a logical network identical to the domain structure of the Windows network and the anti-virus protection system based on versions 5.0 and 6.0 of Kaspersky Anti-Virus for Windows Workstations.

CHAPTER 3. INSTALLING KASPERSKY ADMINISTRATION KIT

Before starting the installation, make sure that the computer meets the software and hardware requirements to the Administration Server and the Administrator's workstation (see section 1.3 on page 9).

MSDE (Microsoft Data Engine), MySQL server or Microsoft SQL server is used to store the Administration Server information. If no MSDE or SQL server is installed, you have to install one of them before installing the Administration Server. In order to do it, you can use the distribution packages you have. In order to install MSDE you can also use Kaspersky Administration Kit distribution package. The MSDE installation procedure from the Kaspersky Administration Kit is discussed in detailed below (see section 3.1 on page 16).

For installation of Kaspersky Administration Kit the local administrator's rights are required for the computer on which the installation is performed.

The setup wizard will offer you to install the application components of Kaspersky Administration Kit (the Administration Server and Administration Console) on the computer on which the setup wizard is run. Such configuration is recommended at the initial stage of creating the centralized administration system.

All the required ports should be open on a host computer for installed application components to work properly. A listing of default ports used by Kaspersky Administration Kit is given in Table 1.

Table 1

Port Number	Protocol	Description
Host Running Administration Server		
13000	TCP and UDP	SSL protocol is used: <ul style="list-style-type: none"> • to receive data from clients; • to connect to update agents; • to connect to slave Administration Servers; • to receive notification of host shutdown.
13292	TCP	Used for connection to mobile devices. ²
14000	TCP	Used: <ul style="list-style-type: none"> • to receive data from clients; • to connect to update agents; • to connect to slave Administration Servers.
18000	HTTP	Used by Administration Server to download data from a Cisco NAC authentication server.
Host Designated as Update Server		
13000	TCP	Used by clients to connect.
13001	TCP	Use by client computers to connect if a host with Administration Server is designated as update agent.
14000	TCP	Used by clients to connect.

² Mobile device is any handheld device where Kaspersky Anti-Virus 6.0 Mobile Enterprise Edition is installed.

Port Number	Protocol	Description
14001	TCP	Use by client computers to connect if a host with Administration Server is designated as update agent.
Client Running Administration Agent		
15000	UDP	Use to receive requests to connect to Administration Server.

3.1. Installing MSDE from the Kaspersky Administration Kit distribution package

Before installing MSDE you must install Microsoft Data Access Components (MDAC) 2.8 or higher (the distribution package is available Microsoft website).

Installation of MSDE from the Kaspersky Administration Kit distribution package to a computer is performed locally.

To install MSDE:

1. Run the executable file in the **MSDE2KSP3** directory on the Kaspersky Administration Kit 5.0 installation CD. The installation wizard will then suggest that you configure settings and run the application. Follow the setup wizard's instructions.
2. First steps are common and include unpacking required files from the distribution package and copying them to the hard drive of your computer, verification of the required software, accepting the license agreement and providing information about the user and the company.
3. Then define the following in the **Installation folder** dialog box:
 - in the **Application modules** field - the folder for installation of the MSDE application files. The default folder is: **<Disk:\Program Files\Microsoft SQL Server**. If this folder does not exist, it will be created automatically.

- in the **Database** field - a folder that will be used to store the MSDE server database. The default folder is also **<Disk:\Program Files\Microsoft SQL Server.**

To select the folders use the **Browse** button.

4. After this, in the **SQL server name** dialog box (see Figure Figure 1) specify the name that will be assigned to this server. By default the name is not created and to address the server the name of the computer on which the server is installed will be used. If you wish to assign a different name, uncheck the **By default** box and enter a new name in the **SQL server name**.

After you have configured the settings, you can review them and start the installation. Once the installation is successfully completed, MSDE will be installed on your computer.

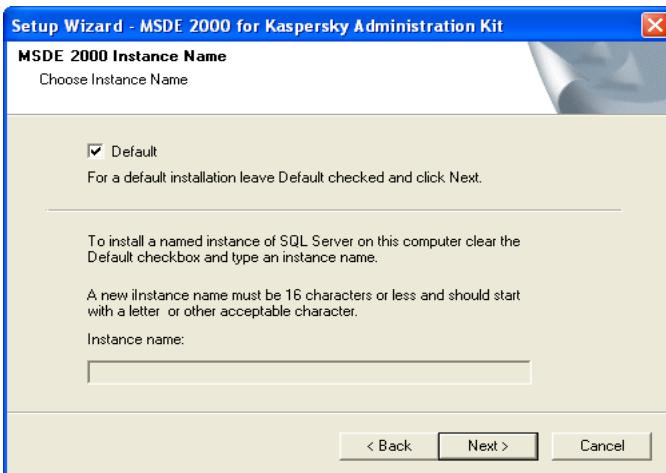


Figure 1. Selecting the server name

3.2. Installing the Administration Server and Administration Console on Local Host

This section describes a local installation of Administration Server and/or Console. If there is even a single Administration Server running on a network, additional servers may be installed using forced installation under the remote installation task. When creating the task, use an Administration Server installation package

To install the Administration Server and / or the Administration Console on local host,

1. Run the **setup.exe** file in installation CD. The installation wizard will then suggest that you configure settings. Follow the setup wizard's instructions.
2. First, the wizard will unpack required files from the distribution package and copy them to the hard drive of your computer, offer you to accept the license agreement and provide information about the user and the company.
3. Then define the folder to be used to install the components. The default folder is: **<Disk:\Program Files\Kaspersky Lab\Kaspersky Administration Kit**. If this folder does not exist, it will be created automatically. To change the folder, use the **Browse** button.
4. After this, select Kaspersky Administration Kit components that you wish to install (see Figure 2):
 - **Administration Server.** Under this option, it can be specified whether standard Kaspersky Lab components to integrate with Cisco NAC are to be installed. If installation is required, check **Kaspersky Lab Posture Validation Server for Cisco NAC**. Parameters for cooperation with Cisco NAC may be configured under properties or Administration Server policies (cf. Kaspersky Administration Server Reference Guide).
 - **Administration Console.**
 - **Network Agent**

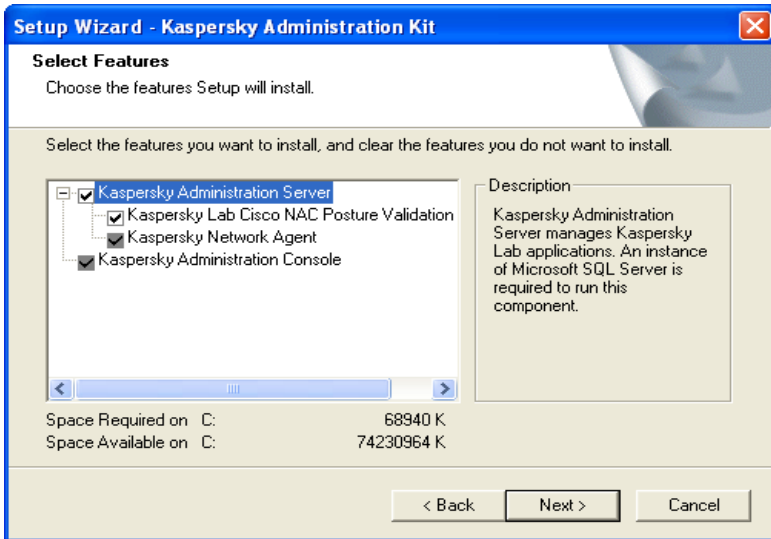


Figure 2. Selecting components for installation

You can select either all components or the Administration Console only. You cannot select installation of the Administration Server without installation of the Console. The default option is to install all components.

A server version of the Network Agent will be installed with the Administration Server. Their joint installation is impossible using a regular version of the Network Agent. If this component is already installed on your computer, remove it and reinstall the Administration Server.

Pay attention to the information displayed in the wizard window:

- in the **Description** field in right section - about the component selected;
- in the bottom section - about the disk space required to install the selected components and available disk space on the drive selected for the installation.

If you selected only the Administration Console, no further steps devoted to configuring the installation settings will be required and you will switch directly to the stage where you only review these settings and start the installation.

5. If you selected installation of the Administration Server, define during the next step under which account the Administration Server will be started as a service on this computer (see Figure 3).

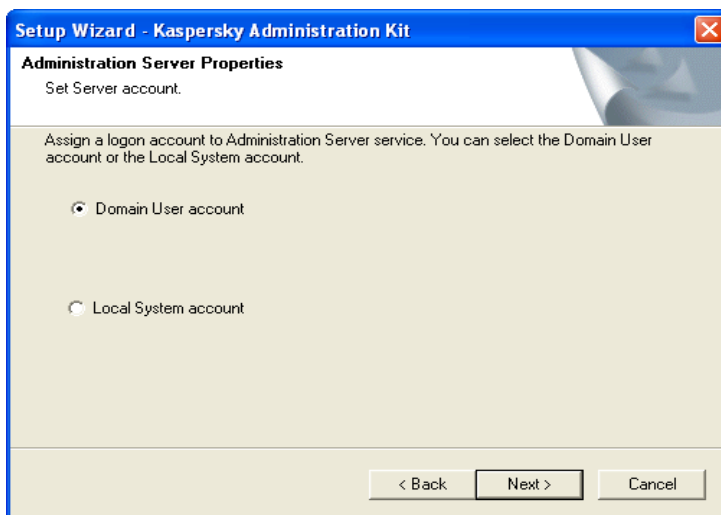


Figure 3. Selecting the account

You can select one of two options:

- **Domain User account** - the Administration Server will be started under the user account included into the domain. In this case the Administration Server will initiate all operations using the rights of this account and during the next stage you will be offered to specify the user whose account will be used.

If a Windows domains structure has been created within the corporate network we recommend selecting the domain administrator's account in order to start the Administration Server. In the future it will allow to avoid configuring additional settings, for example, specifying account of a user who is granted with the domain administrator's rights when creating a deployment (remote installation) task (see section 0 on page 54).

- **Local System account** - the Administration Server will be started under the **System account** with all rights granted to this account. In this case you do not select a user account and will switch directly to the stage where you will have to specify the recourse to store the Administration Server's information database .

For the correct operation of Kaspersky Administration Kit it is mandatory that the account used to start the Administration Server is granted the rights of the administrator for the resource used to store the Administration Server's information database.

6. If you selected a domain's user account to start the Administration Server under, you will be offered to specify such user.

In order to do it, in the **User name** field in the wizard window (see Figure 4) select the user name using the **Browse...** button or enter this name manually out of names registered within the current domain. After this, enter the password used to register the user in the domain.

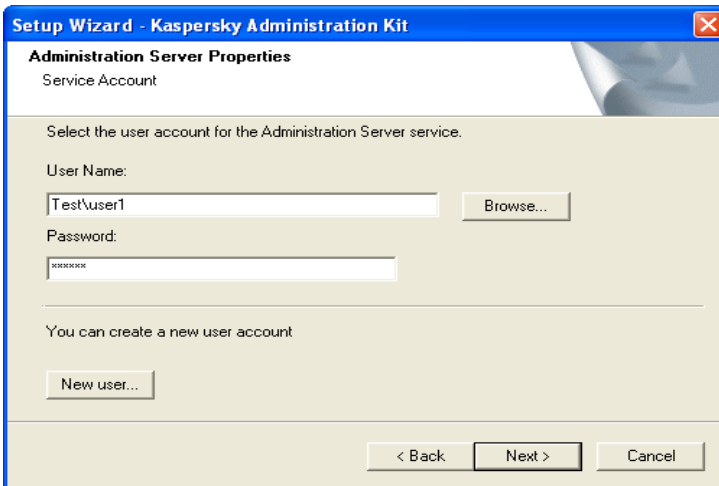


Figure 4. Selecting user

If you selected a user who does not have the domain administrator's rights, the Administration Server will be launched under his account, however the functionality of Kaspersky Administration Kit will be somewhat restricted. For example, it may not have the rights required to execute a deployment task using a launch scenario (see section 0 on page 54) and polling some domains of the Windows network.

For the correct operation of the **Administration server**, the account used to launch it must have the following rights:

- Log on as a service;
- Act as part of the operating system;
- Access this computer from the network;

- Replace a process level token;
- Increase quotas/ Adjust memory quotas for a process.

If the user you selected is a domain administrator, but it does not have the rights listed above, such rights will be granted to this user (see Figure 5).

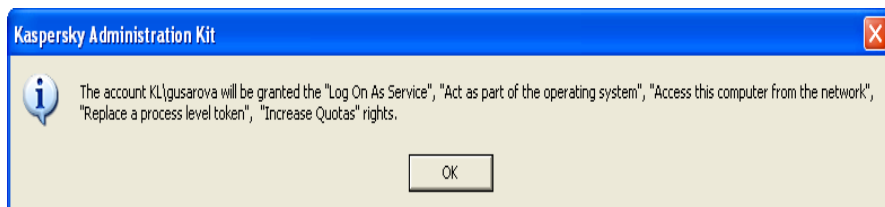


Figure 5. Message about rights granted to the user.

7. During the next stage you will be offered to define resource **Microsoft SQL server (MSDE)** or **MySQL** (see Figure 6), that will be used to store the Administration Server information database.

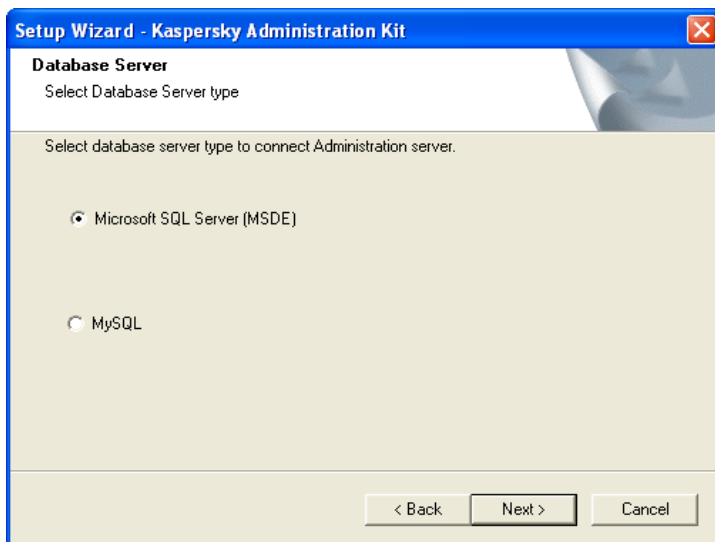


Figure 6. Selecting the database

8. If during the previous stage you selected MSDE or Microsoft SQL server and you are planning to use a server installed within the corporate network to work with Kaspersky Administration Kit, indicate such server's

name in the **SQL server name** and specify the name of the database that will be created to store the Administration Server data in the **SQL server database name** (see Figure 7). The default database name is **KAV**.

Value (**local**) will be automatically assigned to the **Server name** field if an SQL server is detected on the computer from which Kaspersky Administration Kit is being installed. To display the list of all Microsoft SQL servers installed in the network, press the **Browse...** button.

If the Administration Server will be started under the local administrator's account or under the system account, the **Browse** button will not be available.

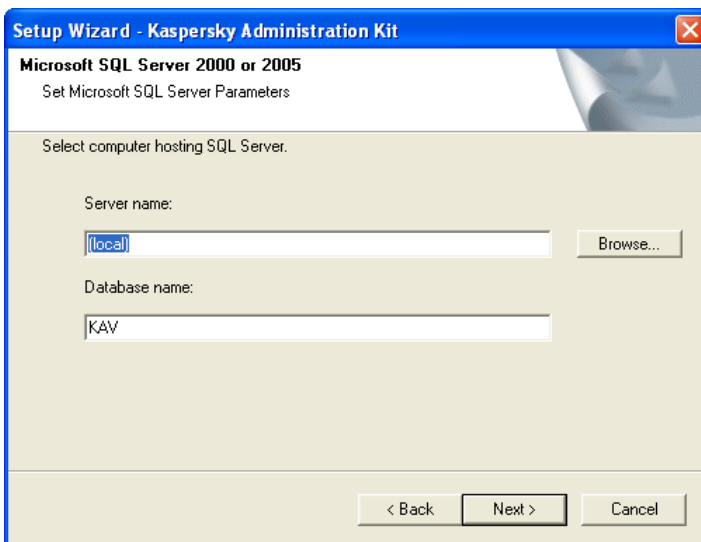
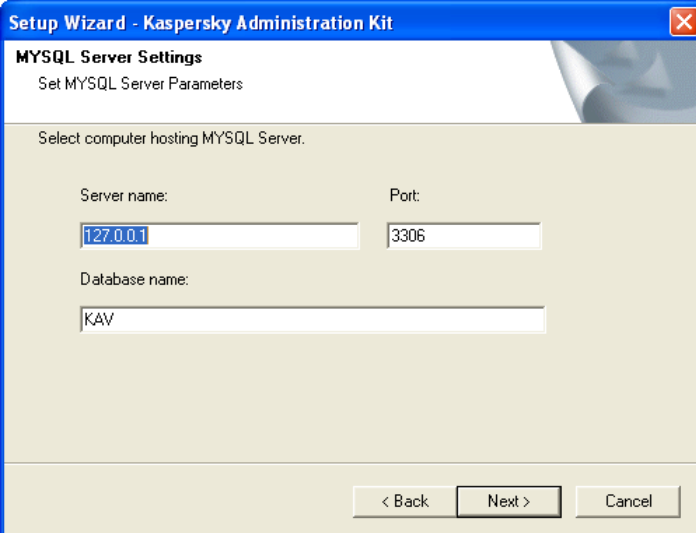


Figure 7. Selecting SQL server

If during the previous stage MySQL server was selected, specify in this window (see Figure 8) its name in the **MySQL server name** field (by default IP address of the computer onto which Kaspersky Administration Kit is being installed will be used) and specify port to be used for connection in the **Port** field (the default port is 3306). In the **MySQL server database name** field specify the database name that will be created to store the Administration Server data (by default the database will be created under name **KAV**).

If during the previous stage MySQL server was selected, specify in this window



Setup Wizard - Kaspersky Administration Kit

MYSQL Server Settings
Set MYSQL Server Parameters

Select computer hosting MYSQL Server.

Server name: 127.0.0.1 Port: 3306

Database name: KAV

< Back Next > Cancel

Figure 8. Selecting MySQL server

If there are no SQL servers in the network and you cannot use them, you have to install one (see section 3.1 on page 16).

If you wish to install an SQL server on the computer from which you are installing Kaspersky Administration Kit, you have to abort the installation and restart it after you have installed the SQL server.

If you install Kaspersky Administration Kit onto a remote computer, it is not required to interrupt the Kaspersky Administration Kit installation wizard. Install the SQL server and return to the Kaspersky Administration Kit installation.

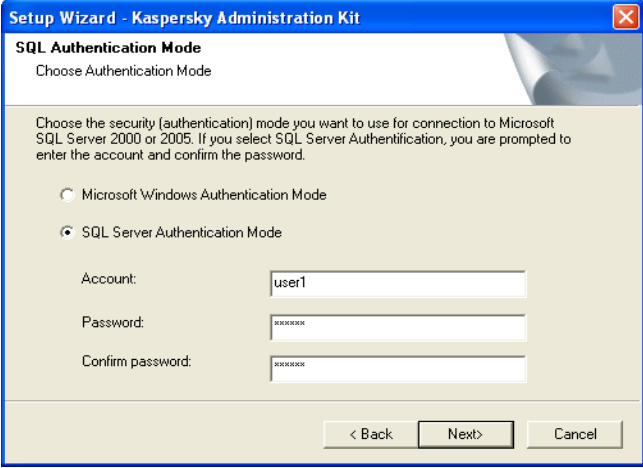
9. During this step you have to define the authentication mode to be used by the Administration Server to connect to the SQL server.

For MSDE or Microsoft SQL server you can select of the following two options (see Figure 9).

- **Microsoft Windows Authentication Mode** - in this case the account used to start the Administration server will be used to verify the rights;

- **SQL Server Authentication Mode** - if you select this option, the account specified below will be used to verify the rights. Fill in the **Account**, **Password** and **Confirm password** fields.

If Administration Server Database is on another computer, you need to choose SQL server authentication mode when installing or updating an Administration Server.



Setup Wizard - Kaspersky Administration Kit

SQL Authentication Mode
Choose Authentication Mode

Choose the security (authentication) mode you want to use for connection to Microsoft SQL Server 2000 or 2005. If you select SQL Server Authentication, you are prompted to enter the account and confirm the password.

Microsoft Windows Authentication Mode

SQL Server Authentication Mode

Account:

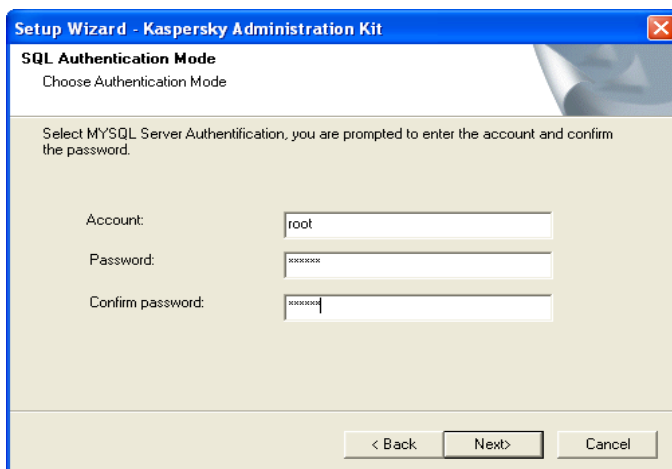
Password:

Confirm password:

< Back Next > Cancel

Figure 9. SQL server authentication mode

For MySQL server indicate the account and the password (see Figure 10).



Setup Wizard - Kaspersky Administration Kit

SQL Authentication Mode
Choose Authentication Mode

Select MYSQL Server Authentication, you are prompted to enter the account and confirm the password.

Account:

Password:

Confirm password:

< Back Next> Cancel

Figure 10. MySQL server authentication mode

10. After this (see Figure 11), specify the location to store the shared folder that will be used:
 - to store files required for remote installation of applications (files will be copied to the Administration Servers when installation packages are created);
 - to store the updates copied from the updates source to the Administration server.

This resource will be public to all users for reading only.

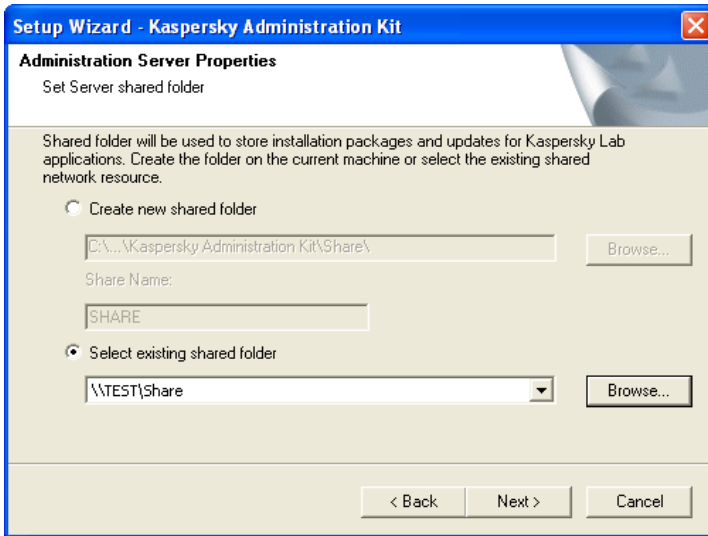


Figure 11. Creating a shared folder

You can select one of the following two options:

- **Create new shared folder** - to create a new folder; you will have to specify path to the folder in the field below.
- **Select existing shared folder** - in order to select a shared folder from the list of existing shared folders.

A public shared folder can be stored either locally, on the computer from which the installation is performed or remotely, on any of the computers included into the corporate network. A shared folder can be specified both using the Browse button, and manually by entering a UNC path (for example, [\\server\KLShare](#)) in the appropriate field.

By default a local folder **KLShare** will be created in the folder specified for installation of the Kaspersky Administration Kit application components.

11. Use the next wizard dialog to specify Administration Server address (cf. Figure 13) by setting:
 - DNS name. This option is used when there is a DNS server on the network which clients can use to obtain Administration Server address.

- NetBIOS name. This option is used where clients obtain Administration Server address through the NetBIOS protocol or if there is a WINS server on the network.
- IP address. This option is used where the Administration Server has a static IP address which will not subsequently change .

If required, check **Allow NetBIOS Name Service in Kaspersky Antivirus 6.0 Anti-Hacker**. This will open UDP port 137 in Kaspersky Antivirus 6.0 Anti-Hacker installed on the host. This port is used to obtain Administration Server IP address.

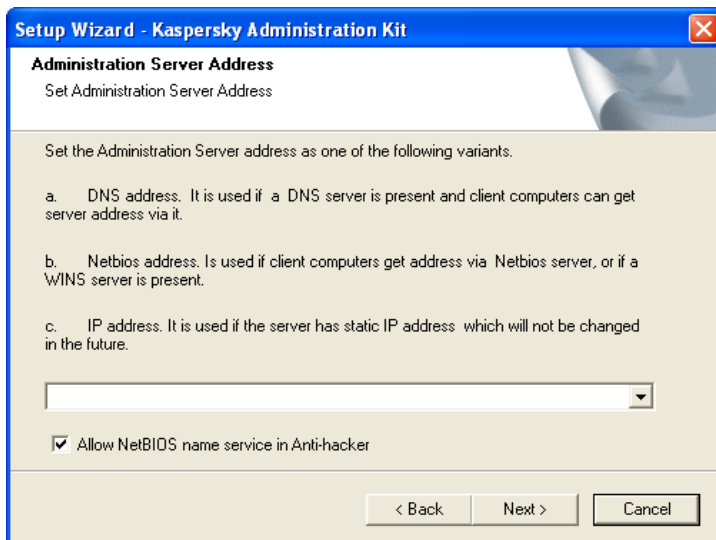


Figure 12. Administration Server Address

12. After this configure settings to be used for connection to the Administration Server (see Figure 13);
 - port number that will be used to connect to the Administration Server. By default port **14000** will be used. If it has been assigned, you can change it.
 - SSL port number that will be used for secure connection to the Administration Server using SSL protocol. By default port **13000** port is used.

If the Administration Server is running Microsoft Windows XP SP 2, then the in-built firewall will block TCP port under numbers 13000 and 14000. Therefore, in order to ensure access, these ports must be opened manually on the host running the Administration Server.

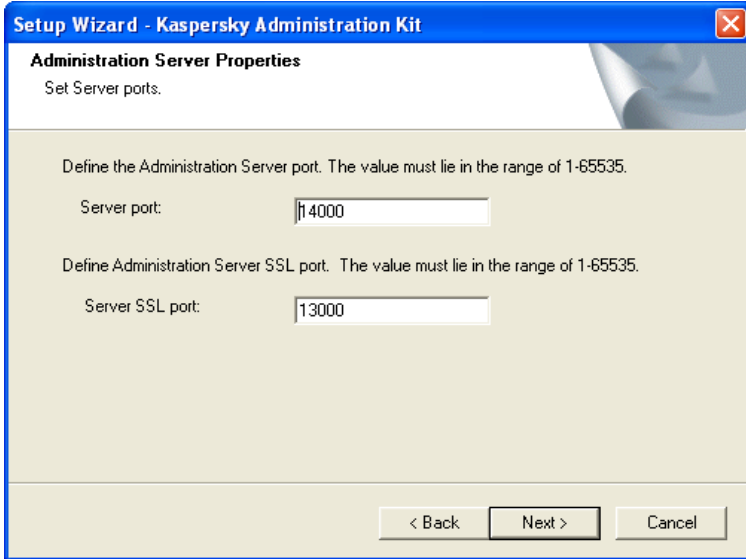


Figure 13. Settings used to connect to the Administration Server

13. In this wizard window (see Figure 14), indicate the method for creation the certificate to be used for authentication of the Administration Server being installed.

Two options are provided:

- **Create new certificate** - select this option if you are installing a new Administration Server. Save a backup copy of the certificate so that later, if required, it would be easier for you to restore the date and structure of the logical network of this Server. In order to do it, check the **Create a backup copy of the certificate** box.
- **Restore certificate** - select this option if you are restoring the Administration server with no backup copy available. In this case you can restore the data and the structure of the logical network of the previous Administration Server.

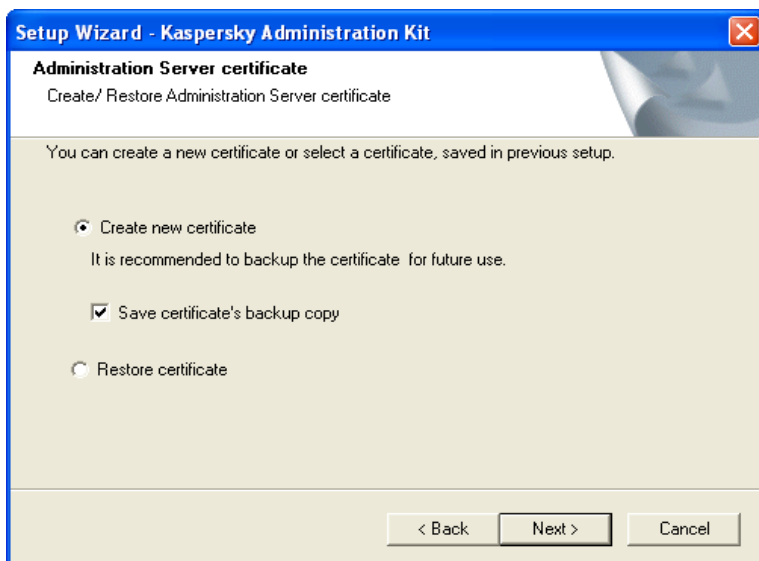


Figure 14. Selecting the method to be used to receive the Administration Server certificate

14. If during the previous stage you selected creation of a new certificate and saving its backup copy, specify the following in the corresponding window (see Figure 15):
 - folder for saving the backup copy of the certificate file;
 - password that will be use for encryption when creating a new certificate and its decryption during its restoration from a backup copy;
 - password confirmation.

In order to be able to restore the data of the Administration Server later, you must save the Server's certificate.

When restoring the certificate you must enter the same password that was used for backup copying. If you enter an incorrect password, the certificate will not be restored.

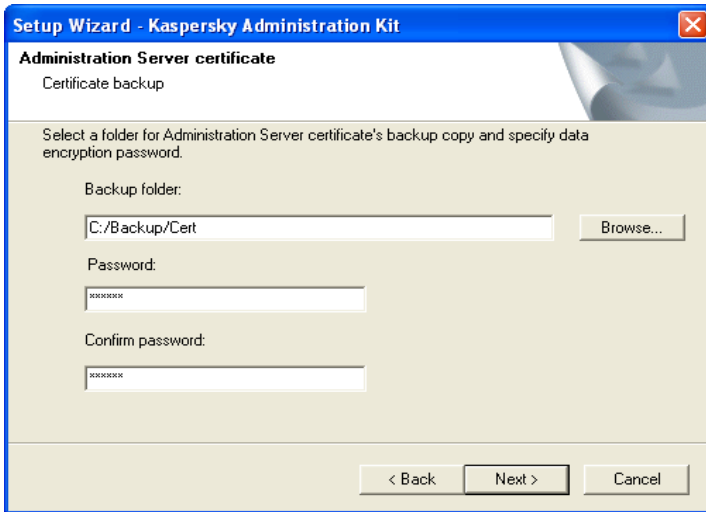


Figure 15. Selecting folder for saving the backup copy of the certificate

If during the previous stage you select the option of restoring the Server's certificate from a backup copy, specify the following in the corresponding window (see Figure 16):

- folder in which the backup copy of the certificate file is saved;
- password that was used for encryption when creating a backup copy of the certificate.

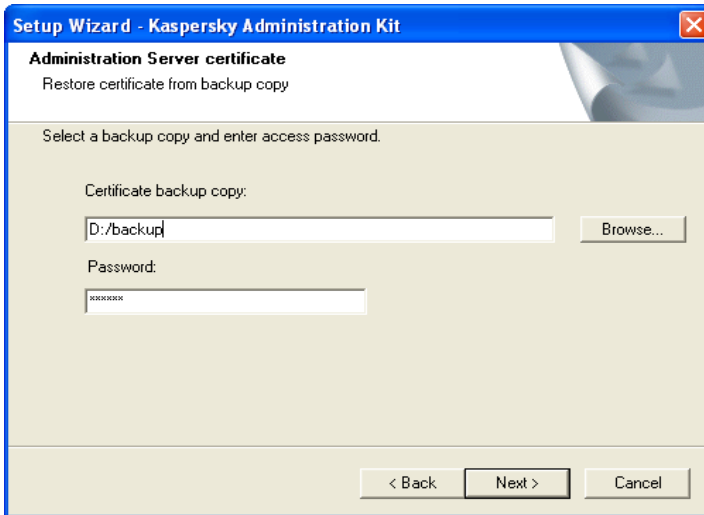


Figure 16. Selecting the folder for storing the backup copy of the certificate.

After you have finished configuring the Kaspersky Administration Kit installation settings, you can review them and start the installation.

After the installation of the Administration Console an icon will appear in menu **Start → Programs → Kaspersky Administration Kit** of your computer. This icon can be used to start the Console.

The Administration Server and Agent will be installed on a host computer as services with attributes listed in Table 2. The table also lists properties of the Kaspersky Lab Posture Validation Server (PVS) for Cisco NAC, which is going to run on the host in question if appropriate components had been installed together with the Administration Server.

Table 2

Property	Administration Server	Kaspersky Lab PVS for Cisco NAC	Administration Agent
Service Name	CSAdminServer	nacserver	klagent
Displayed Service Name	Kaspersky Administration Server	Kaspersky Lab Cisco NAC Posture Validation Server	Kaspersky Network Agent

Property	Administration Server	Kaspersky Lab PVS for Cisco NAC	Administration Agent
Process Name in Windows Task Manager	klserver.exe	klnacserver.exe	klagent.exe
Startup Type	Automatically, at operating system boot.		
User Name	Local Service or user specified.		

A server version of the Network Agent will be installed on the computer together with the Administration Server. It is included into the structure of the Administration Server component and is installed or removed together with it and can only interact with the Administration Server installed locally. You do not have to configure the settings used by the Agent to connect to the Administration Server, as programmatically this connection is implemented based on the assumption that these components are installed on the same computer. Such configuration allows to avoid additional configuration and possible conflicts in the operation of the components if they are installed separately.

A server version of the Network Agent is installed with the same attributes and performs the same application administration functions as the standard Network Agent. It will operate based on the policy of the group into which the Administration Server's computer is included as a client computer, all tasks provided for the Network Agent will be created except the Server change task.

A separate installation of the Network Agent on the Administration Server's computer is not required. Its functions will be performed by the server version.

You can review properties of the following services: **Kaspersky Administration Server**, **Kaspersky Network Agent**, and **Kaspersky Lab Cisco NAC Posture Validation Server**; and monitor their operation using the standard Windows administration tools - **Computer Management** → **Services**. Information about operation of the **Kaspersky Administration Server** service will be registered and saved in the Windows system log on the computer where the Administration Server is installed, in a separate branch of the **Kaspersky Event Log**.

Additionally, groups of local users **KLAdmins** and **KLOperators** will be created on the computer on which the Administration Server is installed. If the Administration Server is run under the account of a user included into the domain, then groups **KLAdmins** and **KLOperators** will be added to the list of groups of the domain users. Change of the list of the groups is performed using standard Windows administration tools.

3.3. Removing Kaspersky Administration Kit components

You can uninstall Kaspersky Administration Kit using both the **Uninstall Kaspersky Administration Kit** option under **Start → Programs → Kaspersky Administration Kit** and the standard Windows **Add / Remove Programs** facility. This will start a wizard that will uninstall all application components (including plugins) from the computer. In the event that you do not request that the wizard remove the shared folder (KLSHare), remove it manually after all the tasks it is needed for are complete.

When you are removing the programs you will be offered to save a backup copy of the Administration Server.

3.4. Updating the application version

In order to update Kaspersky Administration Kit versions 4.x and 5.0 (Planned Update 1 and Planned Update 2) to later versions you have to uninstall the previous version and install a new one as described in this Guide

When updating versions 5.0 (Planned Update 3) and 6.0 to a newer version, data may be recovered out of a backup generated by an earlier version of the application. To accomplish this, we recommend that you follow a procedure described below:

Data restoration during the upgrade to a later application version is supported starting with Kaspersky Administration Kit version 5.0 Maintenance Pack 3.

1. Using the **klbackup.exe** utility create a backup copy of the installed Administration Server's data. This utility is included into the Kaspersky Administration Kit distribution package and after the installation of the Administration Server it is located in the root installation folder. Note that in order to be able to fully restore the Administration Server data you have to save the Server's certificate. This is a mandatory setting for the **klbackup.exe** utility.
2. Run installation of the upgraded version of Kaspersky Administration Kit 6.0 on the computer on which the previous version of the Administration Server and/or Console is installed. Upgrade the component. During the upgrade all data and settings of the previous version of the Administration Server and/or Console will be saved and made available in the new version. Backward compatibility between the new and the old versions of

the Administration Server is supported. The new version of Administration Server is backward compatible with the previous version.

3. In order to upgrade the Network Agent installed on the network computers, create a group or a global task for installation of a newer version of the component. Run the task manually or according to the schedule. After this task is successfully completed, the newer version of the Network Agent will be upgraded.

If you encounter any problems during the installation, you can restore the previous version of Kaspersky Administration Kit using the backup copy of the Administration Server's data created before the upgrading.

If even a single Administration Server is installed, additional servers may be updated using the remote installation task and the Administration Server install package.

CHAPTER 4. INSTALLATION AND REMOVAL OF SOFTWARE ON THE COMPUTERS

Before you start the installation, you must make sure that the software and hardware of the computers meet the corresponding requirements (see section 1.3 on page 9)

Kaspersky Administration Kit allows installation and removal of Kaspersky Lab's applications using the following methods:

- remotely in a centralized way, via the Administration Console;
- locally, individually on each computer.

Connection of the Administration Server with the client computers is ensured by the Network Agent component. Therefore this component must be installed on each computer that will be connected to the remote centralized administration system before the installation of the anti-virus applications. If you use the centralized method to install the applications via the Administration Console, the Network Agent can be installed together with one of the applications.

On the computer on which the Administration Server is installed, only server version of the Network Agent can be used. It is included into the Administration Server structure and is installed and removed together with the Administration Server (see section 3.2 on page 18).
You do not have to install the Network Agent on this computer.

The Network Agent is installed the same way as the applications - that is either remotely or locally.

The Network Agents can differ depending on the Kaspersky Lab's applications for which they are installed. In some cases only local installation of the Network Agent is possible (details see Guides to the corresponding applications). The Network Agent is installed on the client computer only once.

Kaspersky Administration Kit application administration interface is implemented by the corresponding administration plugins. Therefore, in order to access the application administration interface, the corresponding plugin must be installed on the administrator's workstation. In case of the remote installation method, it is installed automatically when the first installation package for the corresponding application is created. In case of a local installed on the client computer, the administration plugin must be installed manually by the administrator.

Under the current version of Kaspersky Administration Kit the following Kaspersky Lab applications may be managed remotely:

- Workstation and file server protection:
 - Kaspersky Antivirus 5.0 for Windows File Servers;
 - Kaspersky Antivirus 6.0 for Windows Servers;
 - Kaspersky Antivirus 5.0 for Windows Workstations;
 - Kaspersky Antivirus 6.0 for Windows Workstations;
 - Kaspersky Antivirus 5.0 Second Opinion Solution;
 - Kaspersky Antivirus 5.7 for Novell NetWare;
- Perimeter defense:
 - Kaspersky Antivirus 5.6 for Microsoft ISA Server 2000 Enterprise Edition.
- Mail server protection:
 - Kaspersky Antivirus 5.5 for Microsoft Exchange Server 2000/2003, Planned Update 1;
 - Kaspersky Security 5.5 for Microsoft Exchange Server 2003, Planned Update 1.

For detailed information on managing the above applications using Kaspersky Administration Kit see relevant application Manuals.

4.1. Remote software installation

Remote software installation can be performed from the administrator's workstation in the main application window of Kaspersky Administration Kit.

Some Kaspersky Lab's applications can be installed only the client computers only locally (details see Guides to the corresponding applications). However, remote administration of these applications using Kaspersky Administration Kit will be available.

In order to perform remote software installation:

1. Create an installation package (see section 0 on page 54). The structure of this package will include files required to install the application and the files that contain settings of the installation package.

Installation package contains file setup.exe using which the local installation of the application in non-interactive mode is performed.

2. Create remote installation task (see section 0 on page 54).

In order to install the application on all computers in the logical network or several administration groups or on specific computers from various groups, you must create a global deployment (remote installation) task.

In order to install the application on all computers of an administration group (including all nested groups and slave servers), you must create a group deployment (remote installation) task.

You can use the deployment wizard (see section 4.2 on page 72) to create either a group or a global task.

The task you create will be run according to the schedule. Application operation settings on each client computer will be configured based on the group policy and the default settings of the application.

You can abort the installation process by manually interrupting execution of the task.

All installation packages created for the Administration Server will be located on the console tree in a special container **Remote Installation**. On the Administration Server these installation packages will be stored in the specified shared folder in the service folder **Packages**.

You can review the properties of the installation package, change its name and settings using the **Properties: <Package Name>** window (see Figure 20). This window opens using the **Properties** shortcut menu command or the analogous item in the **Action** menu.

The installation packages created can be distributed on the slave Administration Servers (see section 4.1.4 on page 50) and on the computers within a group using the updating agents (see section 4.1.6 on page 52).

One installation package can be reused many times to create deployment tasks.

Applications may also be installed in non-interactive mode.

4.1.1. Creating an installation package

in order to create an installation package:

1. Connect to the Administration Server you need.

2. Select in the console tree the **Remote installation** node, open the shortcut menu and select command **Create** → **Installation Package** or use the analogous item in the **Action** menu. This will start the wizard. Follow its instructions.
3. You will be offered to specify the name of the installation package and during the next step - to specify the application to be installed (see Figure 17).

If you are installing an application that supports remote installation via Kaspersky Administration Kit, you have to select the **Create the installation package for Kaspersky Lab's application** option from the drop-down list. Using the **Browse...** button, select file that contains description of the application (file has extension **.kpd** and is bundled with all Kaspersky Lab applications for which remote administration via Kaspersky Administration Kit is supported) or a self-extracting archive of the Kaspersky Lab's application (file has extension **.exe** and can be downloaded from the Kaspersky Lab's website). As the result, fields with the application name and the version number will be automatically filled in.

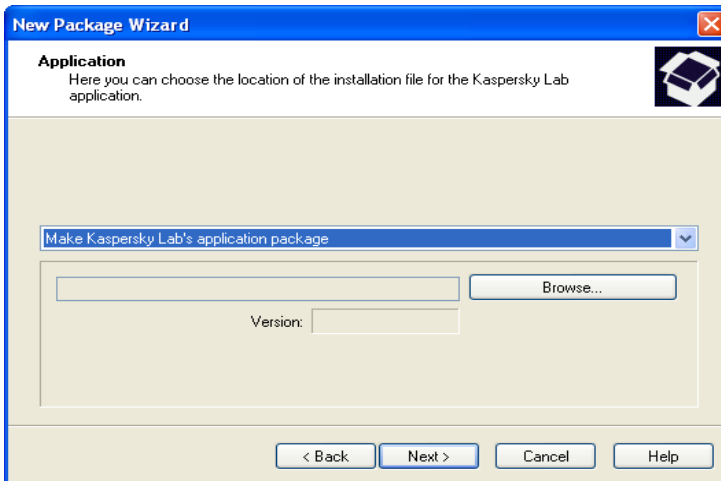


Figure 17. Creating an installation package. Selecting application to be installed

Settings of the installation package will be created by default and will correspond to the application selected to be installed. You can change the settings after the package is created using the package properties review window (see section 4.1.2 on page 41).

If you create an installation package to install other applications (see Figure 18):

- select Create installation package for application specified by the user from the drop-down list;
- indicate the path to the application distribution package using the **Browse** button;
- install the **Copy entire folder into the installation package** box, if the package must contain the entire content of the folder in which the distribution file is located;
- specify the settings used to run the executable file in the entry line provided if such settings are required to install the application (for example, running in non-interactive mode using switch /s).

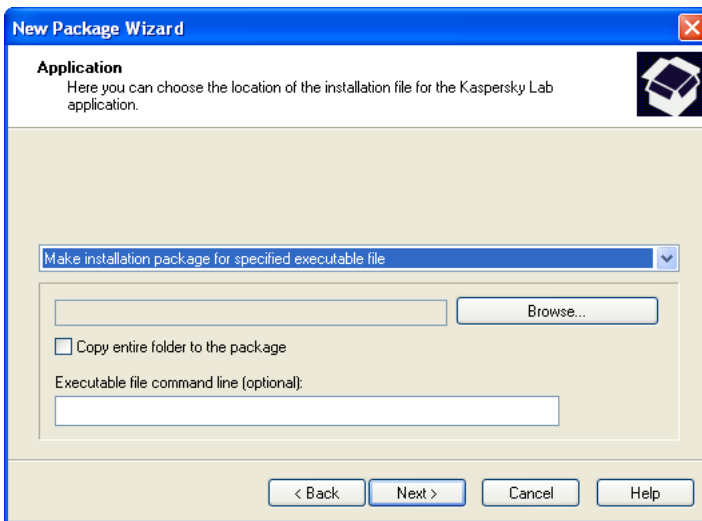


Figure 18. Creating and installation package to install application specified by user.

4. In the next wizard window (see Figure 19), you can specify the license key that will be included into the installation package. In order to do it, press the **Browse...** button and select the required file of the license key (file has extension **.key**)

If you do not wish to include the license key into the installation package, simply press the **Next>** button.

A license key is not required as the installation package for Administration Server and Agent is being generated.

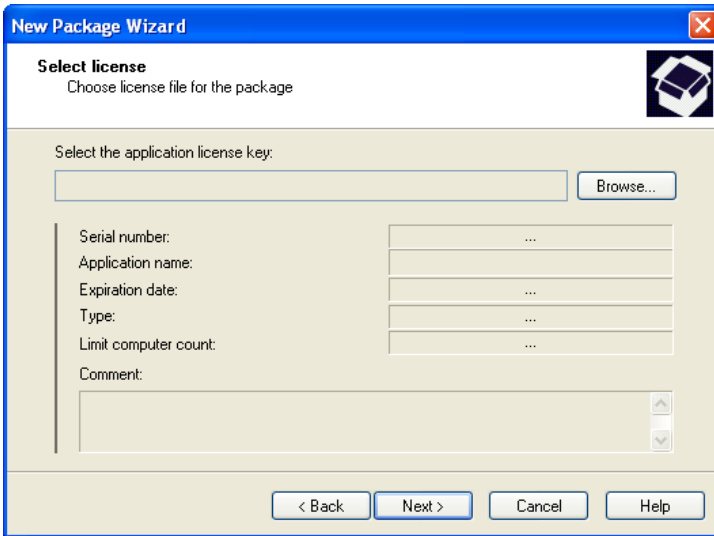


Figure 19. Creating an installation package. Selecting the license key

5. After this the required set of files for the installation of the specified application onto the client computers will be downloaded to shared folder on the Administration Server and a check whether the administration plugin for the selected application is installed on the administrator's workstation will be performed. If such plugin is not installed or its version is older than the version included into the distribution package, the new plugin will be installed and the old plugin will be replaced.

Upon the completion of the wizard, the installation package created will be added to the **Remote installation** node and displayed in the results pane.

4.1.2. Reviewing and configuring the installation package settings

To review the properties of the installation package, change its name and settings:

in the console tree, expand the **Remote Installation** node, select the required installation package in the results pane and use the **Properties** command from the shortcut menu or the analogous command from the **Action** menu.

This will open window **Properties <Installation package name>** see Figure 20) that consists of tabs **General**, **Settings**, **Licenses** and **OS reboot**.

The **General** tab (see Figure 20) includes general information about the package:

- package name;
- name and version of the application for which installation the package has been created;
- package size;
- creation date.

The **Settings** tab (see Figure 21) contains the installation package settings for the application for which installation the package is created. These settings are created by default at the stage of the package creation and if required, you can modify them.

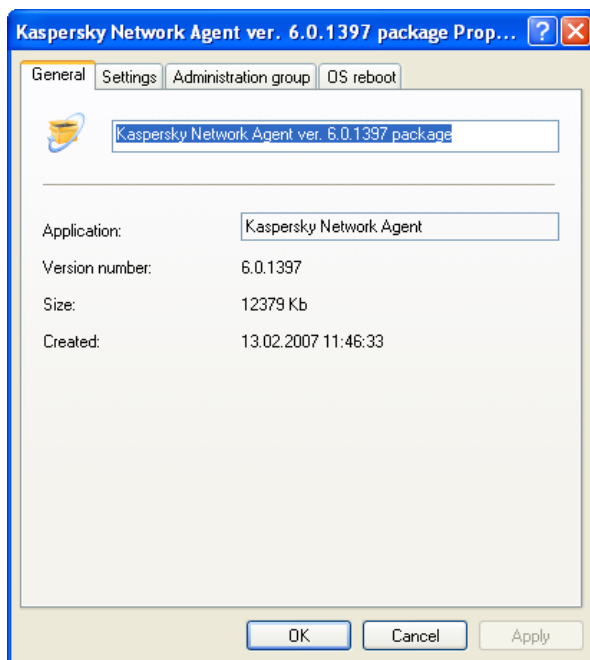


Figure 20. Installation package properties review window
The **General** tab

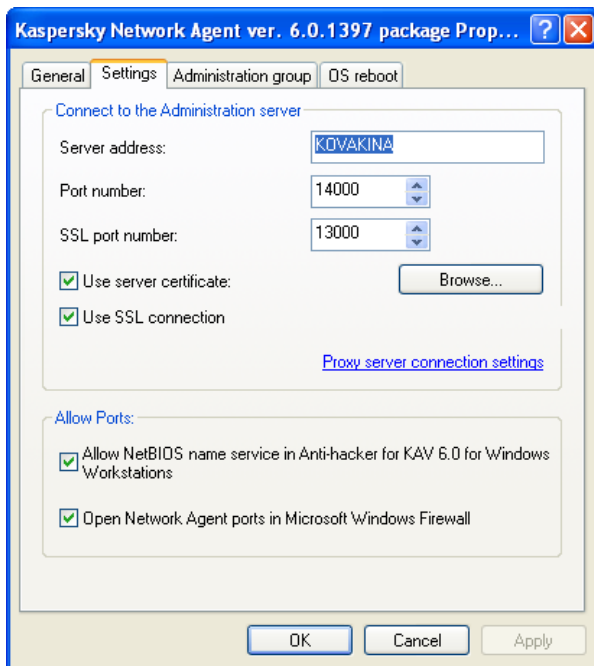


Figure 21. Installation package properties review window
The **Settings** tab

The **License** tab (see Figure 22) contains general information about the license for the application for which installation the package is created.

The **License** tab is not available in the properties of the Network Agent or the Administration Server installation package properties.

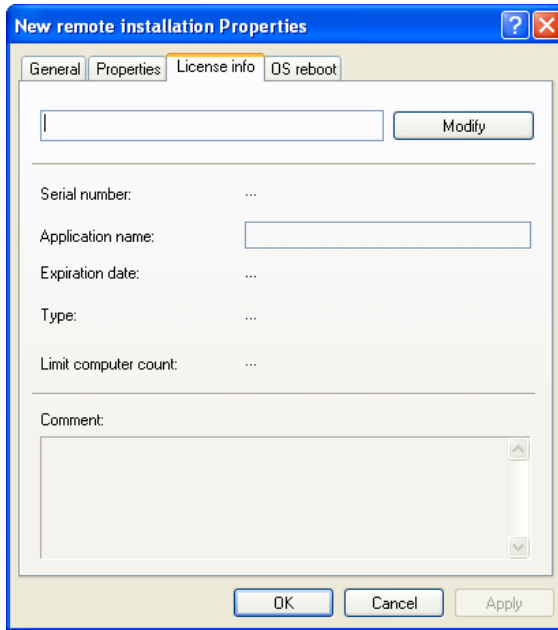


Figure 22. Installation package properties review window
The **License** tab

On the **OS reboot** tab (see Figure 23) you can determine actions to be performed if the computer must be restarted after the installation of the application. You can select one of the following options:

- **Do not restart the operating system**
- **If required, restart the operating system automatically** – this will reboot the operating system only as needed.
- **Prompt user for action** - if this option is selected, you can:
 - create an information message that will be displayed in an entry field to notify the user that the operating system must be restarted.
 - specify a frequency of notifications about the operating system restart if the user cancelled the restart, by checking the **Repeat prompt every (min.)** box and specifying the interval for the message to be displayed;

- o specify automatic restart of the computer's operating system if it is not performed by the user within the specified time interval starting with the moment the application has been installed. In order to do it, check the **Force the restart in (min.)** box and specify the time interval.

If a locked computer needs to be rebooted, check **Close Running Applications Automatically**. By default this option is unchecked.

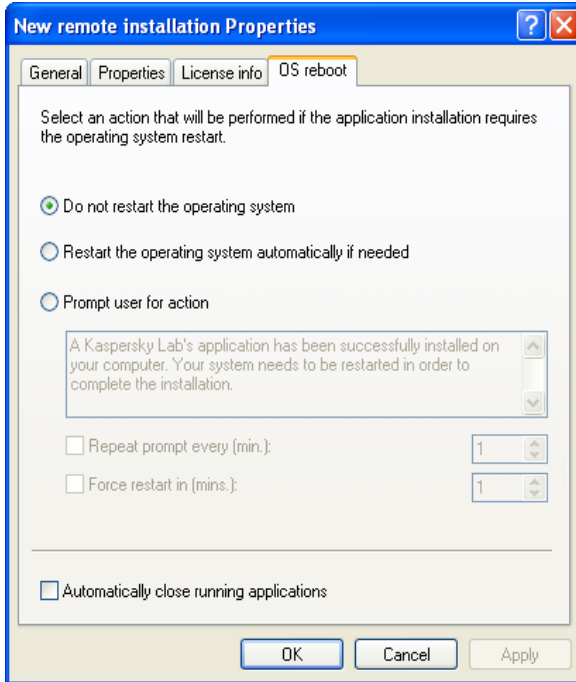


Figure 23. Installation package properties review window
The **Operating System restart** tab

4.1.3. Creating and configuring the Network Agent installation package

The installation package for the remote installation of the Network Agent does not have to be created manually. It is created automatically during the installation of Kaspersky Administration Kit and located in the **Remote installation** node.

If the package for the remote installation of the Network Agent has been deleted, then in order to create it again, select file **klagent.kpd** located in the NetAgent folder of the Kaspersky Administration Kit distribution package to be used as the file that contains the description

The settings of the Network Agent installation contain a minimum set of settings required to ensure the functioning of the component immediately following its installation. The values of the settings match the values of the default application settings. If required, these can be changed using the **Settings** and the **Administration Group** tabs of the installation package properties window.

The **Settings** tab (see Figure 21) contains settings used by the Network agent after it is installed on the client computers to connect to the Administration Server (by default, values of the current server will be used during the creation).

- Address of the computer on which the Administration Server is installed.
- Number of port used for unsecured connection to the Administration Server. By default port **14000** is used. If this port is busy, you can change it.
- Number of port used for secure connection to the Administration Server using SSL protocol. By default port **13000** is used.

Only decimal representation is allowed.

- Certificate file for authentication of the access to the Administration Server. The value of this setting is determined by the **Use the Server Certificate** box.

If the box is not checked by default, the certificate file will be automatically obtained from the Administration Server when the Agent connects to it for the first time.

If the **Use Server Certificate** box is checked, authentication will be performed based on the certificate file specified using the **Browse** button. This file has extension **.cer** and is located in the **Cert** folder of the Kaspersky Administration Kit installation folder. You can change the certificate file by selecting the file you need using the **Browse** button.

- Which port will be used by the Network Agent to connection to the Server: simple or secure. The value of this setting is determined by the **Use SSL connection** box. If the box is checked, the connection is performed via a secure port using SSL protocol, if the box is unchecked, the connection is performed via an unsecured port.
- The proxy server connection settings. If a proxy server is used by the Network Agent to connect to the Server, check the **Use proxy server**

box. After this press the **Settings** button and in the window that will open enter the proxy server address, user name and the password.

- Opening UDP Port 137 used to obtain Administration Server IP address in **Kaspersky Antivirus 6.0 Anti-Hacker**. Check **Enable NetBIOS in Kaspersky Antivirus 6.0 Anti-Hacker**.
- Adding a UDP port required by the Administration Agent to the Microsoft Windows firewall exceptions list. Check **Open Administration Agent Ports on Microsoft Windows Firewall**.

After the installation of the Network Agent you can change the values of the settings used to connect to the Administration Server using the policy and the application's settings.

If you remotely reinstall the Network Agent on the client computer the values of the settings used to connect to the Server and the Administration server certificate will be replaced with new ones.

The **Administration Group** tab (cf. Figure 25) is used to define a subgroup of the **Network** group into which computers will be added after the Network Agent has been installed on them. You can select of the following options:

- add computers to folders **Corresponding to the computer position in the Windows network**: domain or a work group (this option is selected by default);
- add all computers **In group** specified in the entry field. If you select this option, enter the name of the folder in the field below. If the **Network** group does not contain such folder, it will be created (you can also indicate the name of any existing folder in the **Network** group).

This folder will be used to store all computers newly detected in the network; even if a computer had previously been detected by the Administration Server and put into the folder corresponding to its position within the network before the installation of the Network Agent. Computers detected in the network prior to the installation of the Network Agent will remain in their old positions in the **Network** group.

After the installation of the Network Agent you can not change the folder to store the computers in the **Network** group as this setting is not included into the policy and the application settings.

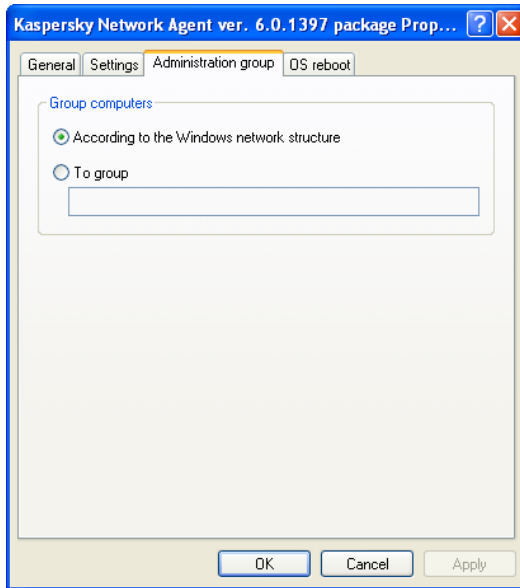


Figure 24. Administration Agent Installation Package Properties Windows. **Administration Group** Tab

The Network Agent is installed on the computer as a service with the following set of attributes:

- service name **KLNAgent**;
- displayed name Kaspersky Network Agent;
- automatic start at the operating system startup;
- with the **Local system** account.

You can review properties of the **Kaspersky Network Agent** service, start it, stop it and monitor its operation using the standard Windows administration tools - **Computer Management** → **Services**.

4.1.4. Creating and Configuring Administration Server Installation Package

When creating an Administration Server installation package as a file with description, select file **ak6.kpd**, located in the root directory of the Kaspersky Administration Kit distribution.

The properties of the Administration Server installation package are shown on two tabs: **General** (cf. Figure Figure 20) and **Reboot OS** (cf. Figure Figure 23). The other properties are the same as Administration Server default settings.

4.1.5. Creating a task for distribution of the installation package on the slave Administration Servers

In order to create the task for distribution of the installation package on the slave Administration Servers:

1. Connect to the Administration Server you need.
2. Select the **Global tasks** node in the console tree, open the shortcut menu and select the **New → Task** command or use the analogous item in the **Action** menu. This will start the wizard. Follow its instructions.
3. For the Kaspersky Administration Kit application select the **Packages retranslation task** task type.
4. In the next wizard window (see Figure 25) select which installation packages must be distributed. Select one of the following options:
 - **All installation** packages.
 - **Selected installation packages**. In this case check boxes next to the names of the required installation packages in the table below.

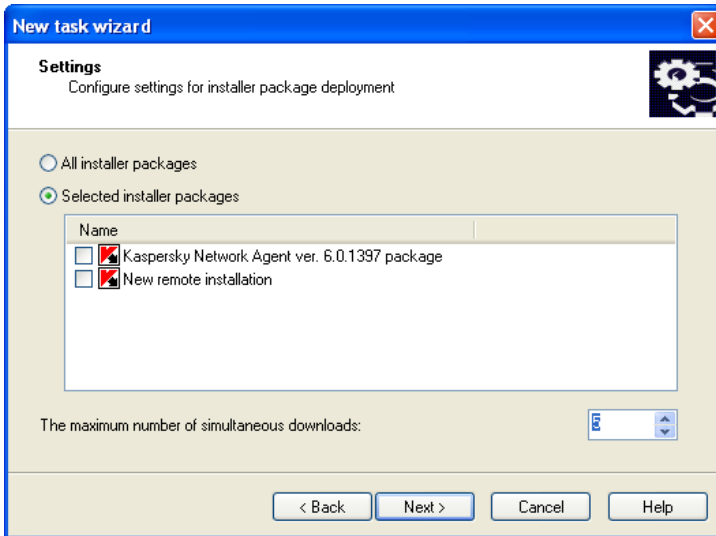


Figure 25. Creating a set of installation packages

Specify the required value in the The maximum number of simultaneous downloads:.

5. In the next wizard window (see Figure 26) check boxes next to the names of the slave Administration Servers to which the installation packages must be distributed.

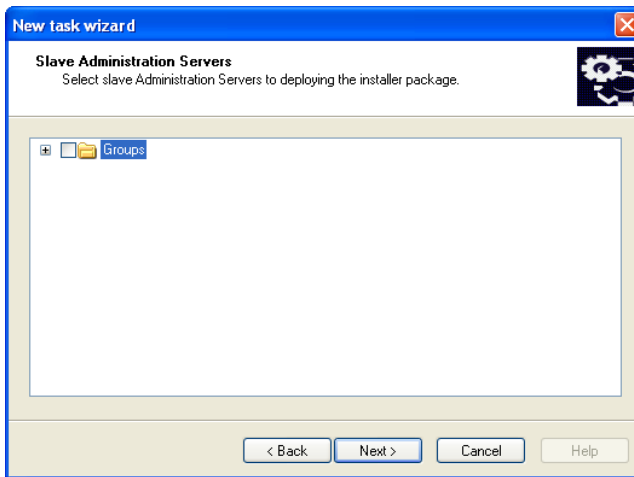


Figure 26. Selecting slave Administration Servers

6. In the next wizard window specify the task launch schedule (details see section 0 on page 54).
7. To exit the wizard when it is completed, press the **Finish** button.

4.1.6. Distribution of the installation packages within a group using network agents

In order to distribute installation packages within a group, you can use updating agents. The updating agents receive installation packages and updates from the Administration Server and save them in the Kaspersky Lab's application installation folder.

The location of the folder that contains the updates and the installation packages cannot be changed; its size cannot be restricted.

Later the installation packages will be distributed to the client computers using the multi-address delivery. Delivery of the new installation packages within a group is only performed once. If at the moment of the delivery a client computer was disconnected from the corporate logical network, then when the installation task is run the Network Agent will automatically download the required installation package from the updating agent.

In order to create the list of the updating agents and configure them to distribute installation packages to computers within a group,

1. Connect to the required Administration Server.
2. Select the required group in the console tree, open the shortcut menu and select the **Properties** command or use the analogous item in the **Actions** menu.
3. In the group properties window that will open, on the **Updating Agents** tab (see Figure 27) create the list of computers that will act as the updating agents within the group, using the **Add** and the **Remove** buttons.

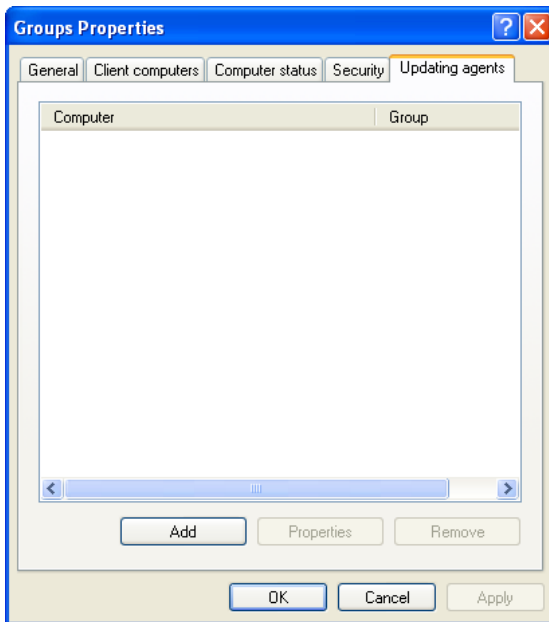


Figure 27. The group properties window.
The **Updating Agents** tab

4. Edit the updating agent's settings. In order to do it, select the agent in the list and press the **Properties** button. In the **<Updating agent name> properties** window that will open (see Figure 28) do the following:
 - specify the number of the port used by the client computer to connect to the updating agent. The default port number is **14001**. If this port is being used, you can change it;

- specify the number of the port used by the client computer to securely connect to the updating agent using SSL protocol. The default port number is **13001**;
 - check box **Use multiaddress IP delivery** and fill in fields **Multicast IP Address** and **Multicast IP Port Number**.
5. Press the **Apply** or the **OK** button.

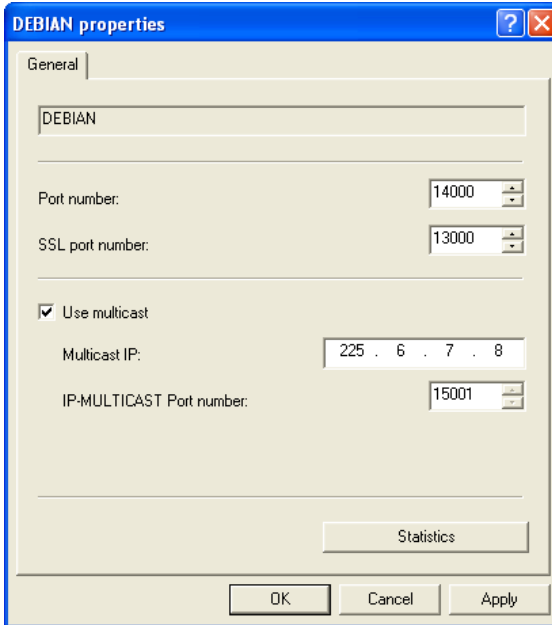


Figure 28. Updating agent properties window

When this task is executed, remote installation of software on the client computers is performed using one of the two methods: **forced installation** or **installation using the startup scenario**.

Forced installation allows performing the remote installation of software on the specific client computers within the logical network. When the task is run, the Administration Server will copy from the shared folder a set of files required to install the application to each client computer in the temporary folder and launches the installer application on each computer. In order to successfully perform the forced installation task the Administration Server must have the rights of the local administrator on the client computers within the logical network. This method is recommended for installation of applications onto computers running

Microsoft Windows NT/2000/2003/XP that support such ability or onto computers running Microsoft Windows 98/Me on which the Network Agent is installed.

If the connection between the Administration Server and the client computer is established via Internet or is protected by a firewall, shared folders cannot be used to transfer data. In this case the files required to install the application to the client computer can be delivered by the Network Agent. The Network Agent is installed on such computers locally.

The second method - **installation using the startup scenario** - allows to assign a remote installation task to a specific user (or several users') account. As the result of the task execution, a record about launching the installer application will be entered into the startup scenario for the selected users. The installer application is located in the shared folder on the Administration Server. In order to ensure successful task execution, the account under which it is run or the Administration Server must have the right to modify the startup scenarios in the domain controller database. As the results of the user registration with the domain an attempt will be made to install the application on the client computer from which the user has registered. This method is recommended for installation of the Kaspersky Lab's applications onto the computers running MS Windows 98/Me.

In order to ensure successful execution of the remote installation task using the startup scenario, users for which changes are made in the scenarios, must have the local administrator's rights on their respective computers.

Group tasks for remote software installation onto the client computers are executed using the forced installation method only. When creating a global task, you can select the method you require: the forced installation or installation using the startup scenario.

In order to create a global task for remote installation using the forced installation method:

1. Connect to the required Administration Server.
2. Select the **Global tasks** node in the console tree, open the shortcut menu and select the **New / Task** command or use the analogous item in the **Action** menu. This will start the task creation wizard. Follow its instructions.
3. Specify the task name.
4. When selecting the application and the task type (see Figure 29), specify values **Kaspersky Administration Kit** and **Remote application installation** respectively.

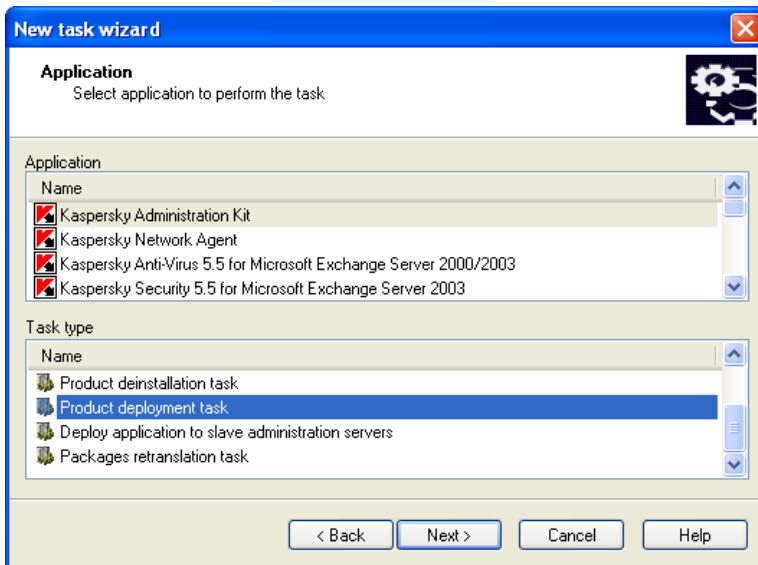


Figure 29. Specifying the task type

5. After this, specify the installation package that will be installed during the execution of this task (see Figure 30). Select the required package from the packages created for the particular Administration Server or create a new package using the **New...** button.

Some applications that support administration via Kaspersky Administration Kit can be installed on the computers only locally. Detailed information see Guides to the corresponding applications.

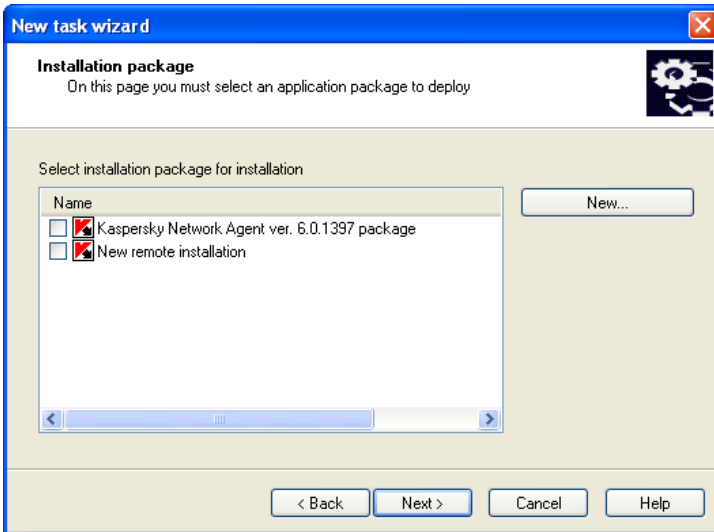


Figure 30. Selecting the installation package for installation

6. During this stage select the **Push install** option (see Figure 31)

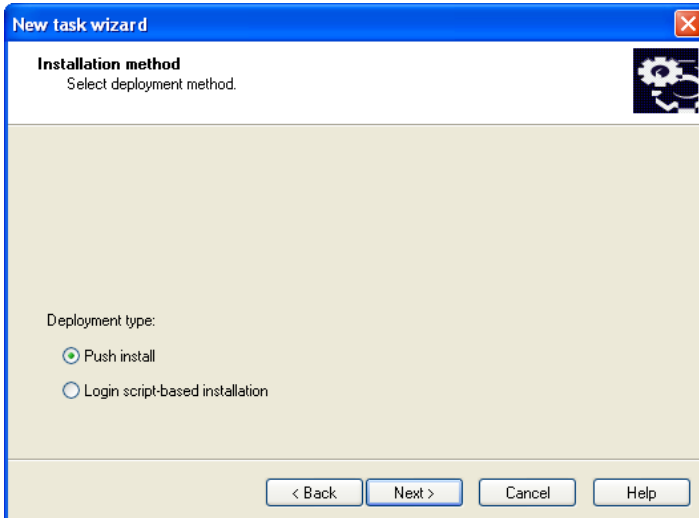


Figure 31. Selecting installation method

7. In this wizard window (see Figure 32) you will be offered to determine additional installation settings.
- Whether the application must be reinstalled if it has already been installed on the computer.

Check the **Do not install application if it is already installed** box in order to prevent repeated installation (by default the box is checked). In this case for the computers on which the application is installed locally or as the result of previous scheduled launch of the remote installation task, the task will not be launched.

If the box is unchecked, the remote installation task will be launched by scheduled until the maximum number of attempts to install the application has been reached.

- To specify the method for delivery of the files required to install the application on the client computers.

In order to do it, perform the following in the **Downloading the installation package** group of fields:

- Check the **Using Microsoft Windows resources from public access folder** box if you wish that the transfer of the files required to install the application to the client computers is performed using Windows tools and the shared folders (by default this box is checked).
 - Check the **Using Administration Agent** box so that the files are delivered to the client computers by the Network Agent installed on each computer (by default this box is checked).
 - In the **The maximum number of simultaneous downloads** field specify the maximum number of client computers that can download information from the Administration Sever.
- Specify the number of attempts to perform the installation in case of a scheduled task launched by entering the required value in the **Number of attempts** field. Repeated attempts are made in case of an error during the execution in the course of the previous installation.

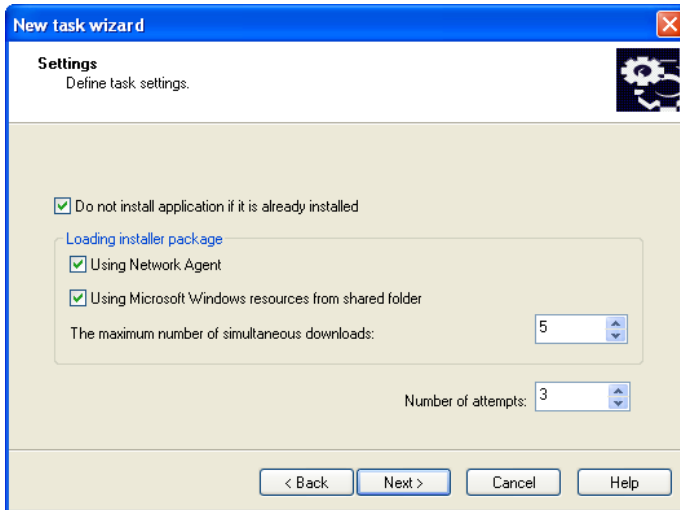


Figure 32. Additional installation settings

8. During this step (see Figure 33) you will be offered to install the Network Agent together with the application.

We recommend that you use the joint installation in order to reduce load on the Administration Server. In order to do it check the **Install along with Administration Agent** box and check box next to the name of the required installation package. If required, create a new installation package using the **Create** button.

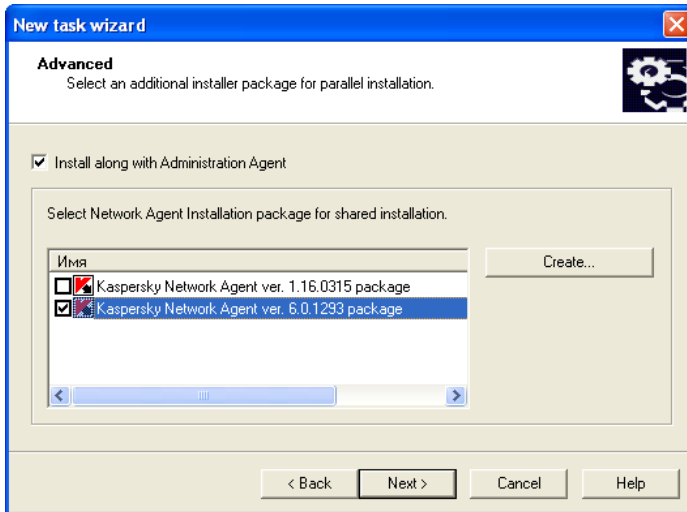


Figure 33. Selecting joint installation with the Network Agent

9. Determine the method to select the computers on which the task will be created (see Figure 34):
 - **Based on data obtained in a Windows network poll.** In this case computers for installation will be selected based on the data received by the Administration Server based on the corporate Windows network polling.
 - **Based on manually entered host addresses.** In this case computers for installation will be selected manually.

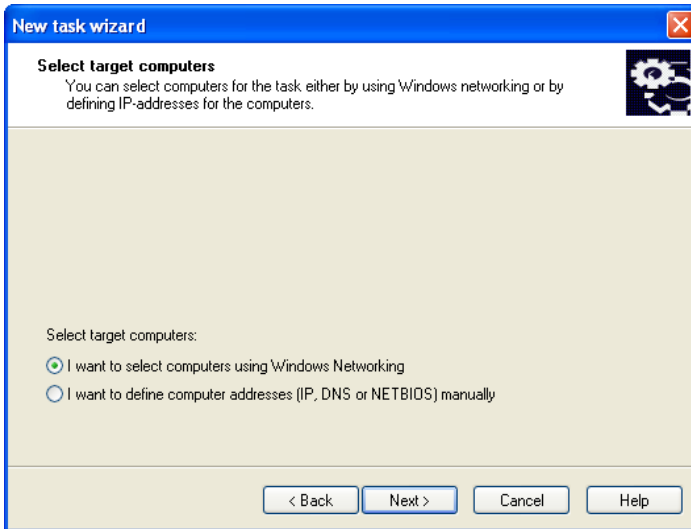


Figure 34. Selecting the method to be used to select the client computers

If computers are selected based on the data received as the result of the Windows network polling, the list will be created in the wizard window (see Figure 35) and will be performed in the same way as when adding computers to the logical network (details see Reference Book for Kaspersky Administration Kit). You can select either the computers of the logical network (the **Groups** folder) or computers that have not yet been included into the logical network (the **Network** folder).

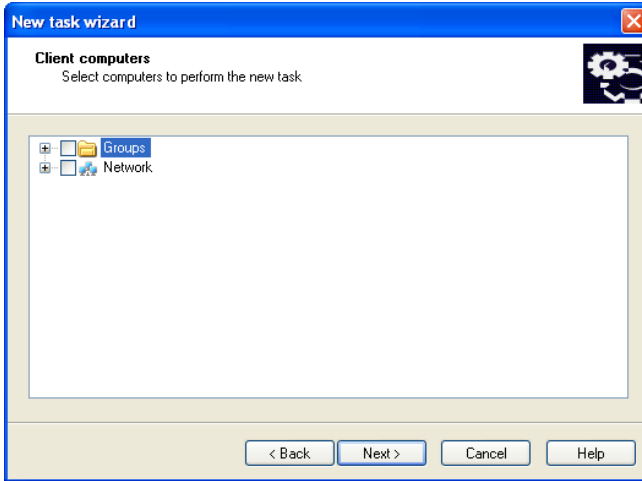


Figure 35. Creating the list of computers for installation based on the Windows network data

If you select computers manually, then the list is created by entering NETBIOS or DNS names, IP addresses (or a range of IP addresses) of the computers or by importing the list from a *txt* file in which each address must be entered in a new line (see Figure 36).



Figure 36. Creating the list of computers for installation based on IP addresses

10. In the next wizard window specify under which account the deployment task will be launched on the computers (see Figure 37).

The account must have the administrator's rights for all computers on which you plan to perform remote software installation.

When installing the software on the computers included in various domains, between such domains and the domain in which the Administration Server is working trusted relationship must exist.

Select one of the following options:

- **Default account** - if the Administration Server is run under the domain user's account (see section 3.2 on page 18) and this account has rights required to install the software.
- **Specified account** - if the Administration Server is run under the system account or if the Administration Server's account does not have the rights required to launch the deployment task.

In order to remotely install the software on the computers not included into the domain, launch the remote installation task under the account of a user who has the administrator's rights on these computers.

In the fields provided below specify the attributes of the user whose account conform to the required conditions.

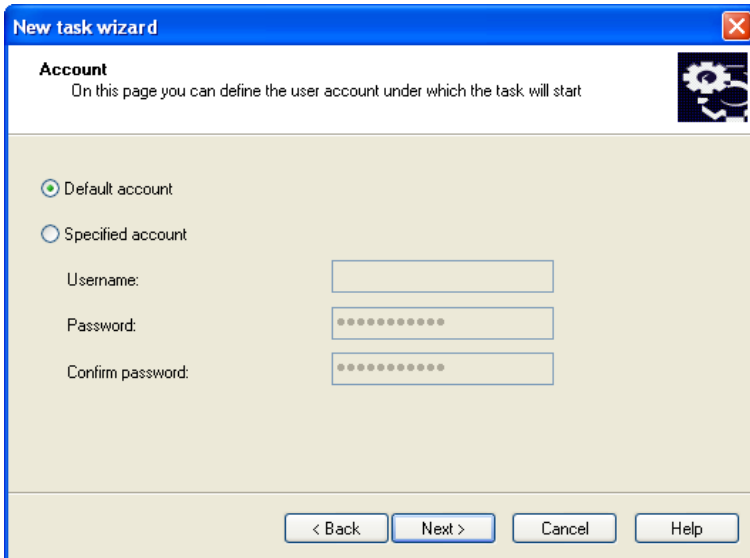


Figure 37. Selecting the account

11. Then create the schedule to launch the task (see Figure 38).

- Select the required task launch mode from the **Scheduled launch** drop-down list:
 - **Manually**
 - **Every N hour(s)**
 - **Daily**
 - **Weekly**
 - **Monthly**
 - **Once** (in this case the deployment task will only run once on the computer irrespective of the result of its execution).
 - **Now** (immediately following the creation of task and completion of the wizard).
 - **Upon completion of another task** (remote installation task will not start until after a specified task exits)

- Configure the schedule settings in the group of fields based on the selected mode (details see Reference Guide for Kaspersky Administration Kit).

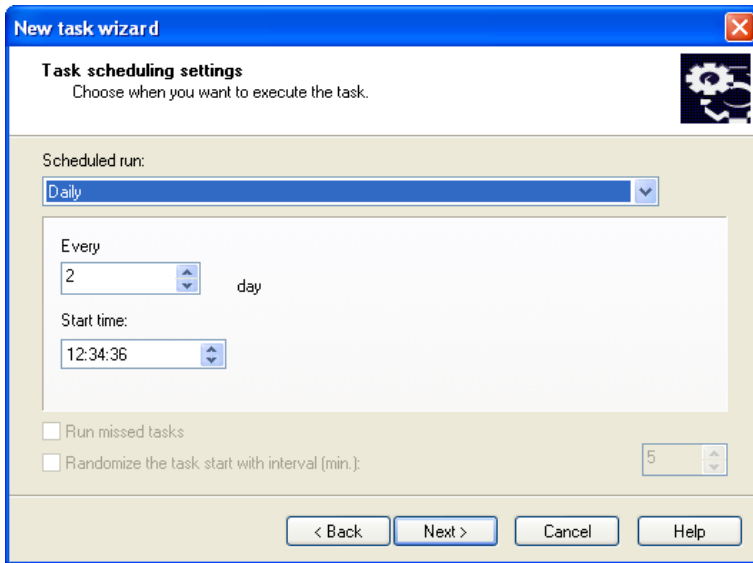


Figure 38. Daily task launch

In order to create a global deployment task using the startup scenario:

1. Connect to the required Administration Server.
2. Select the **Global tasks** node in the console tree, open the shortcut menu and select the **New / Task** command or use the analogous item in the **Action** menu. This will start the task creation wizard. Follow its instructions.
3. Specify the task name.
4. When selecting the application and the task type (see Figure 29), select **Kaspersky Administration Kit** and **Application remote installation** respectively.
5. In the next window (see Figure 30) specify the installation package to be used for the installation. This is performed the same way as with the forced installation method (see above).
6. After this select the **Installation using the startup scenario** option (see Figure 31)

- In the next wizard window (see Figure 36) select accounts of users for which the startup scenario must be changed.

When the installation task is started, Kaspersky Administration Kit checks whether a startup script is specified for any other users in addition to those selected. If that is the case, installation will not proceed. Appropriate error information will be written out to the log file.

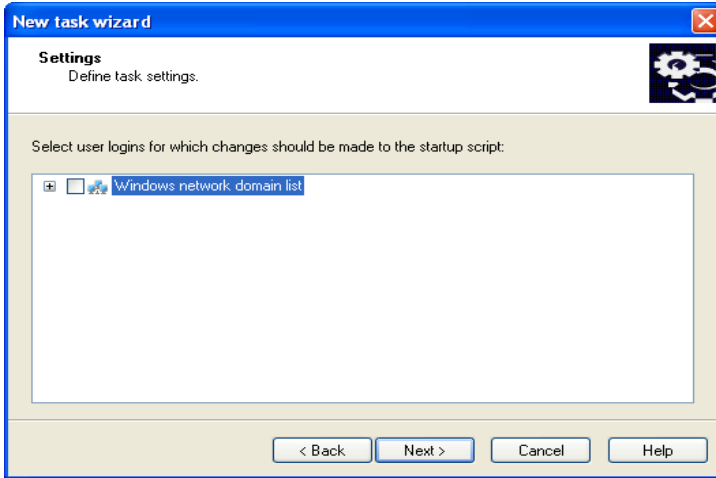


Figure 39. Selecting accounts

- During the next step of the wizard (see Figure 37), similarly to using the forced installation method (see above),
- In the **Task** launch schedule (see Figure 38) create a schedule the same way as it is created if the forced installation method is used (see above).

After the wizard is complete, the deployment task you created will be added to the **Global tasks** node and displayed in the results pane. If required, you can modify its settings (details see section 4.1.7 on page 67).

In order to do it,

select the **Remote installation** node in the console tree, select the installation package required in the results pane, open the shortcut menu and select the **Install** command or use the analogous command from the **Action** menu. This will launch the deployment task creation wizard described above, however, this wizard will not include the task type and installation package selection steps. Follow its instructions.

Alternatively you can launch the group deployment task creation wizard.

In order to do it,

select the **Groups** node in the console tree, open the shortcut menu and select the **Install** command or use the analogous command from the **Action** menu. This will launch the group deployment task creation wizard described above, however, this wizard will not include the task type and computer group selection steps. Follow its instructions.

4.1.7. Configuring the deployment task

Deployment tasks are configured the same way as any task (details see Reference Book for Kaspersky Administration Kit). Provided below is a detailed discussion of settings specific for this type of tasks provided on the **Settings** tab.

If you are editing a task that will perform forced installation (see Figure 40), you can:

- determine whether you have to reinstall the application if it is already installed on the client computer;
- specify the method to be used to deliver the files required to install the application to the client computer and specify the maximum number of simultaneous connections;
- specify the number of attempts to perform the installation if the task is run based on schedule.

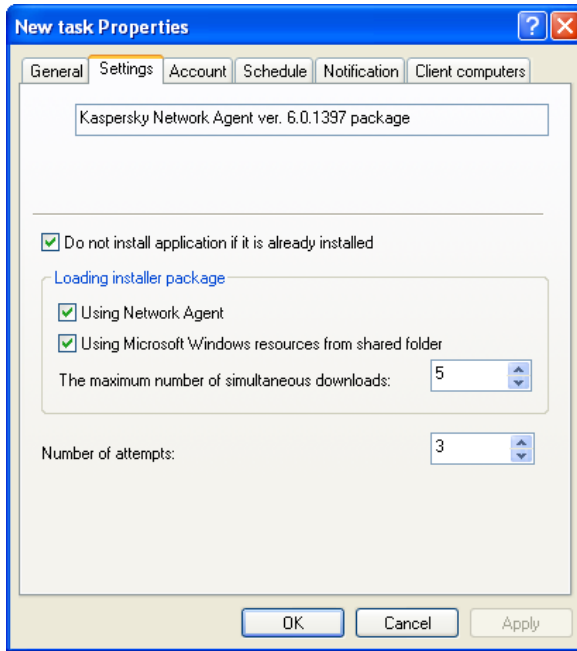


Figure 40. Configuring a deployment task
Push installation method

When configuring a deployment task using a startup scenario, you can use the **Settings** tab to change the list of accounts of users for whom the startup scenario will be modified (see Figure 41). To edit the list use the **Add** and the **Remove** buttons.

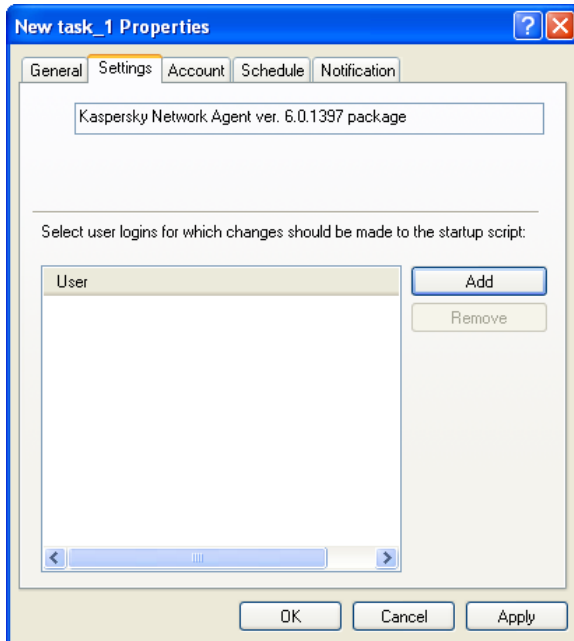


Figure 41. Configuring a deployment task using the startup scenario.

4.1.8. Deploying application to slave administration servers

This task enables you to install and update software on slave servers

Before creating the task make sure that an installation package is on all the servers. Use **Package retranslation task** to send the package to server (see section 4.1.5).

To create application deployment to slave servers task:

1. Connect to the required Administration Server.
2. Select the **Global tasks** node in the console tree, open the shortcut menu and select the **New / Task** command or use the analogous item in the **Action** menu. This will start the task creation wizard. Follow its instructions.
3. Specify the task name.

4. When selecting the application and the task type (see Figure 29), specify values **Kaspersky Administration Kit** and **Deploy application to slave administration servers**.
5. Specify the installation package that will be installed during the execution of this task
6. Check the **Do not install application if it is already installed** box in order to prevent repeated installation (by default the box is checked).
7. This step is not available for a global task. Select **Slave Administration Servers** (Figure. 42) and make up a list of slave servers

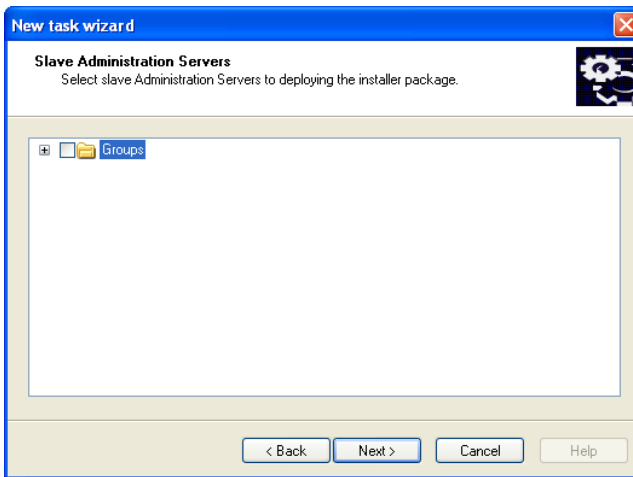


Figure 42. Creating a list of slave administration servers

8. Then create the schedule to launch the task

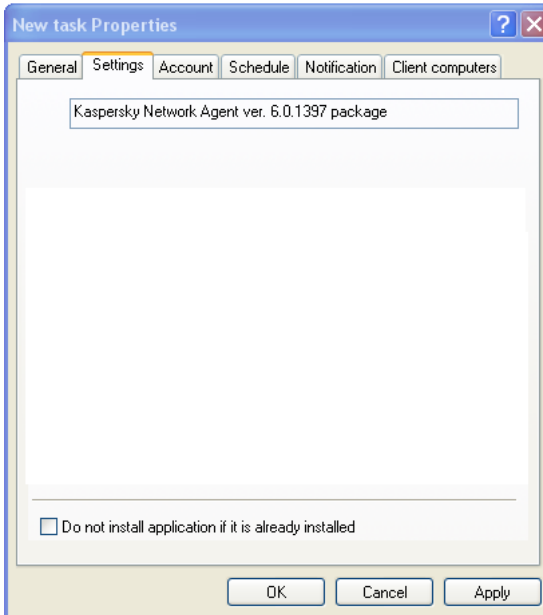


Figure 43. Application Deployment to slave administration servers task. Settings tab.

4.1.9. Remote software removal

In order to remotely remove the software:

Create a task similarly to creation of a deployment task (see section 0 on page 54); select **Remote application removal** as the task type and select the required Kaspersky Lab's application from the **Application to be removed** drop-down list in the **Application** window (see Figure 44). In order to remove a third-party application, check the **Third-party application** and select the application to be removed.

The drop-down list contains the list of applications detected on the computers of the logical networks after the Network Agent had been installed on these computers.

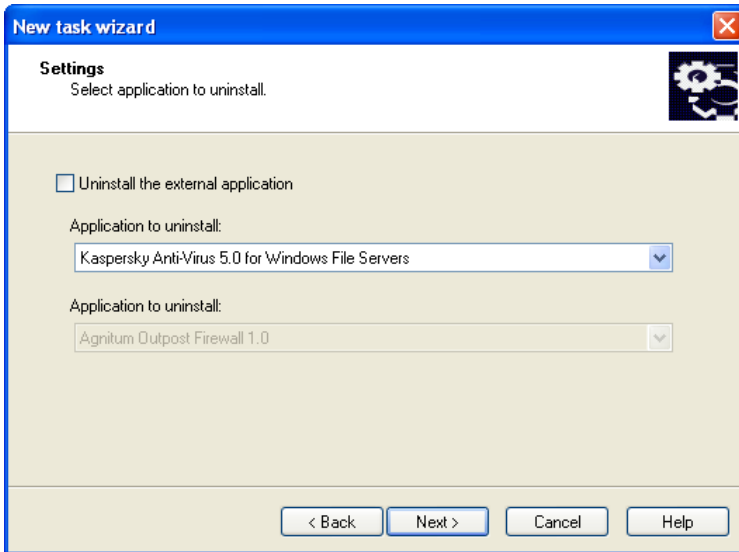


Figure 44. Selecting an application to be removed

The task you created will be run according to the schedule.

4.2. Deployment wizard

You can use deployment wizard to install Kaspersky Lab's applications. This wizard allows performing application deployment using the forced installation method using installation packaged created or directly from the distribution package.

The wizard performs the following:

- creation of an installation package to install the application (if such package has not been installed earlier). The package is stored in the **Remote installation** node under the name that matches the name and the version of the application and can be used to install the application later.
- creation and launching of global and group deployment tasks. The task created will be located in the **Global tasks** or **Group tasks** folder of the group for which the task was created and can be manually run later. The name of the task matches the name of the package for the application installation: **Installation <Name of the selected installation package>**.

In order to install application using the deployment wizard:

1. Connect to the required Administration Server.
2. In the console tree of the main Kaspersky Administration Kit application window select the node corresponding to the required Administration Server, open the shortcut menu and select the **Deployment wizard** command or use the analogous command in the **Action** menu. This will run the wizard. Follow its instructions.
3. In the window that will open (see Figure 45) specify the installation package that will be installed. If you are installing the application from a distribution package and/or if the installation package has not been created, create a new installation package. In order to do it press the **New...** button; this will open the installation package creation wizard (see section 4.1.1 on page 38).

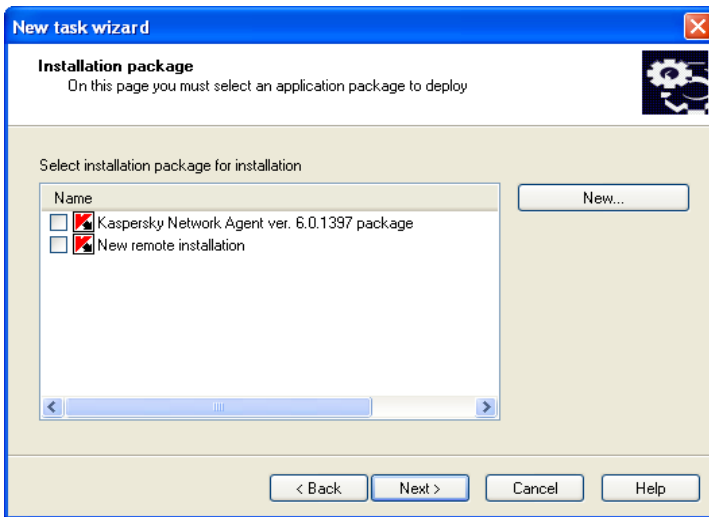


Figure 45. Selecting an installation package

4. In the next wizard window, if required, specify the Network Agent installation package to be jointly installed (details see section 0 on page 54).
5. In the wizard window (see Figure 46) determine on which computers the application will be installed. In order to do it, select one of the options:

- **Install the application onto selected computers**, if you select this option, then after the wizard is complete a global application deployment task will be created.
- **Install application onto computers in the administration group** - as the result of the wizard's work, a group task will be created.

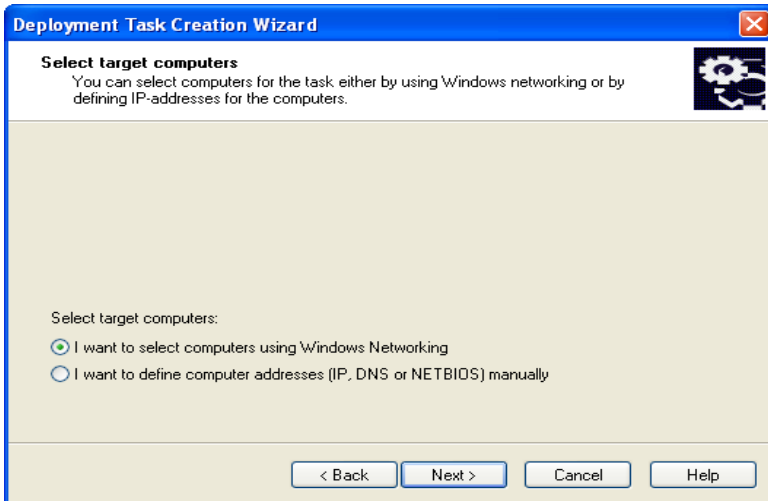


Figure 46. Selecting a task type

6. Then if you are creating a group task, specify a group on whose computers the application will be remotely installed (see Figure 47), or select computers for the installation. If the application must be installed on all client computers within the logical network, select the **Groups** group.

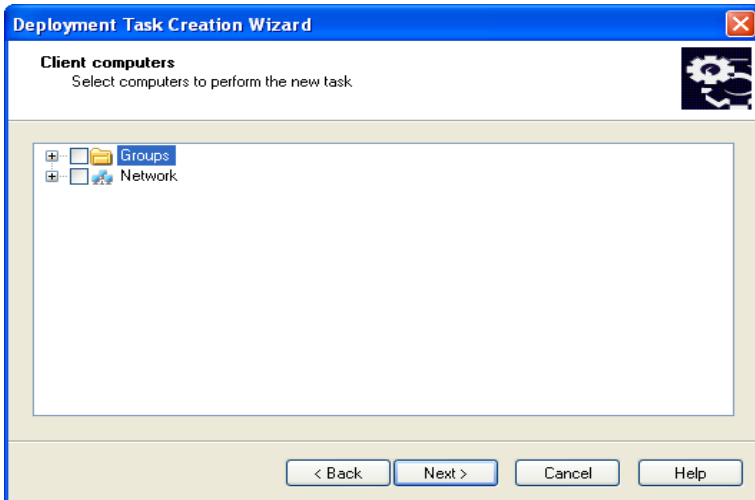


Figure 47. Selecting a group

7. Then determine under which account the deployment task will be run on the computers (details see section 0 on page 54).

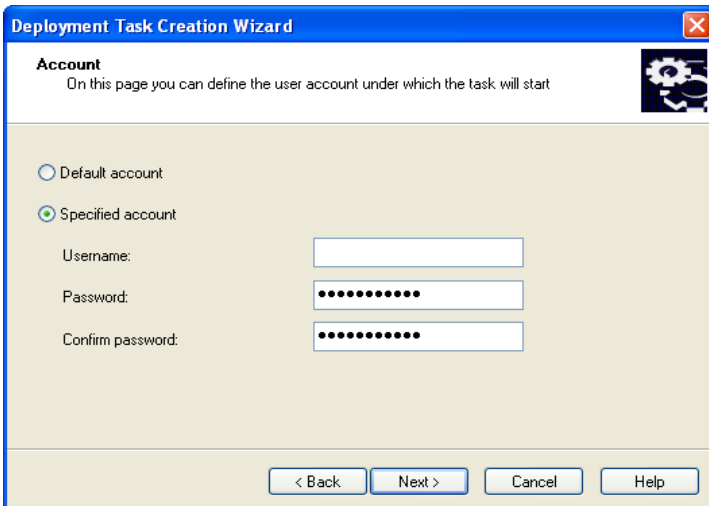


Figure 48. Selecting a user's account

8. After this a window will open that will display the process of distribution and execution of the deployment task on the computers of the selected group (see Figure 49). You can switch to the final window of the wizard without waiting for the process to be completed. In order to do it, press the **Next** button. You can view detailed information about the results of the task execution on each computer using the **History** button.

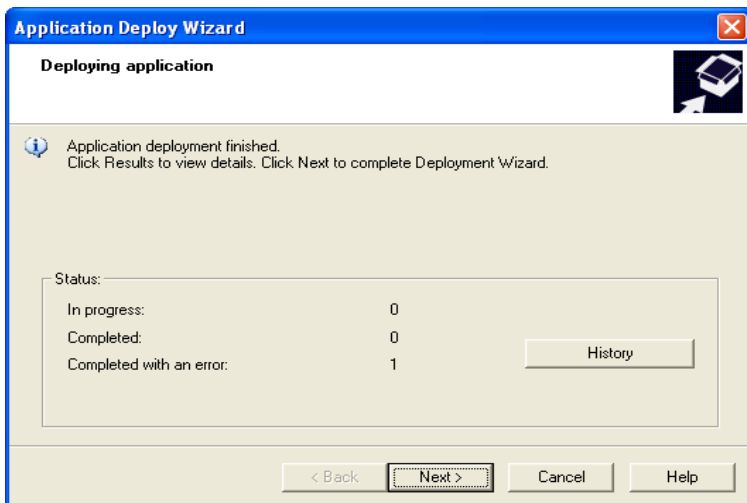


Figure 49. Deployment task execution

4.3. Local software installation

The local software installation is performed individually on each computer. In order to perform local installation you must have the administrator's right for the local computer.

Some applications that support administration using Kaspersky Administration Kit can be installed on computers only locally. Details see Guides to the corresponding applications.

General procedure for the software installation during local deployment of the anti-virus protection system can be as follows:

- install the Network Agent and configure the connection between the client computer and the Administration Server (see section 4.3.1 on page 77);

- install the required applications on the computer that will be included into the anti-virus protection system according to the description in the corresponding Guides;
- install the administration plugin for each of the installed Kaspersky Lab's applications into the administrator's workstation (see section 4.3.2 on page 82).

Kaspersky Administration Kit support local application installation in non-interactive mode based on the files created during installation package creation (see section 4.3.3 on page 83).

4.3.1. Local installation of the Network Agent

In order to locally install the Network Agent on the computer:

1. Run file **setup.exe** (or **setup.msi**) located on the distribution CD of the Kaspersky Administration Kit application in folder **NetAgent**. The installation process is facilitated by the wizard. The wizard will offer you to configure the installation settings. Follow its instructions.
2. First steps of the installation process are the usual procedure and involve unpacking required files from the distribution package and copying them on the hard drive of your computer, accepting the license agreement and providing information about the user and the company.
3. Then you have to define the Network Agent installation folder. The default installation folder is **Program Files\Kaspersky Lab\NetworkAgent**. If such folder does not exist, it will be created automatically. To change the folder use the **Browse...** button.
4. In the next wizard window (see Figure 50) you will have to configure settings used by the Network Agent to connect to the Administration Server. In order to do this define the following:
 - address of the computer on which the Administration Server is or will be installed. The computer's IP address or name in the Windows network can be used as the computer address. Alternatively, you can select the computer using the **Browse** button.
 - whether UDP Port 137, used to obtain Administration Server IP address needs to be opened in Kaspersky Antivirus 6.0 Anti-Hacker. If so, check **Enable NetBIOS Name Service in Kaspersky Antivirus 6.0 Anti-Hacker**.

- the port number using which the Network Agent will connect to the Administration Server. By default port **14000** will be used. If it has been assigned, you can change it. Only decimal representation is allowed.
- port number that will be used for secure connection to the Administration Server using SSL protocol. By default port **13000** port is used. If it has been assigned, you can change it. Only decimal representation is allowed. In order to make sure that the connection is using a secured port (using SSL protocol) check the **Use SSL to connect to server** box.

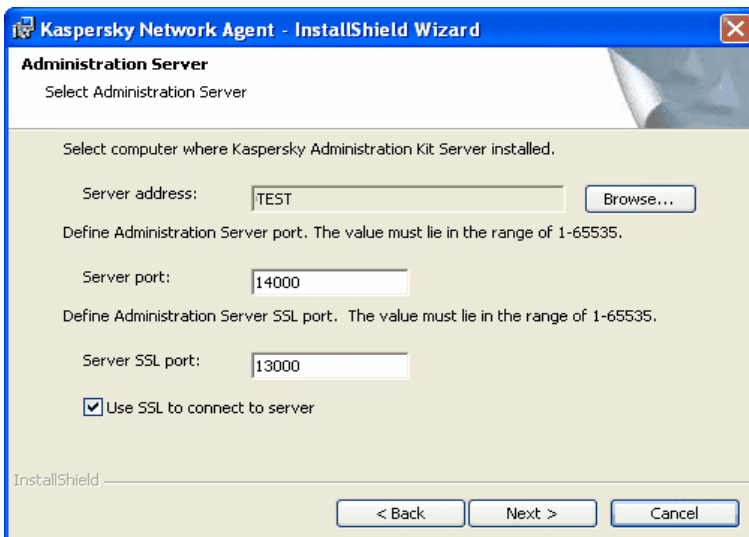


Figure 50. Configuring settings used to connect to the Administration Server

5. If the Network Agent connects to the Server via a proxy server (see Figure 51), configure the corresponding connection settings:
 - Check the **Use a proxy server to connect to the Administration Kit Server** box and enter the address and the name of the port to connect to the proxy server. Only decimal notation is allowed (for example: **Proxy address:** proxy.test.com; **Port:** 8080).
 - If a password is used to access the proxy server, fill in the **Proxy login** and the **Proxy password** fields.

If no proxy server is used, skip this step by pressing the **Next** button.

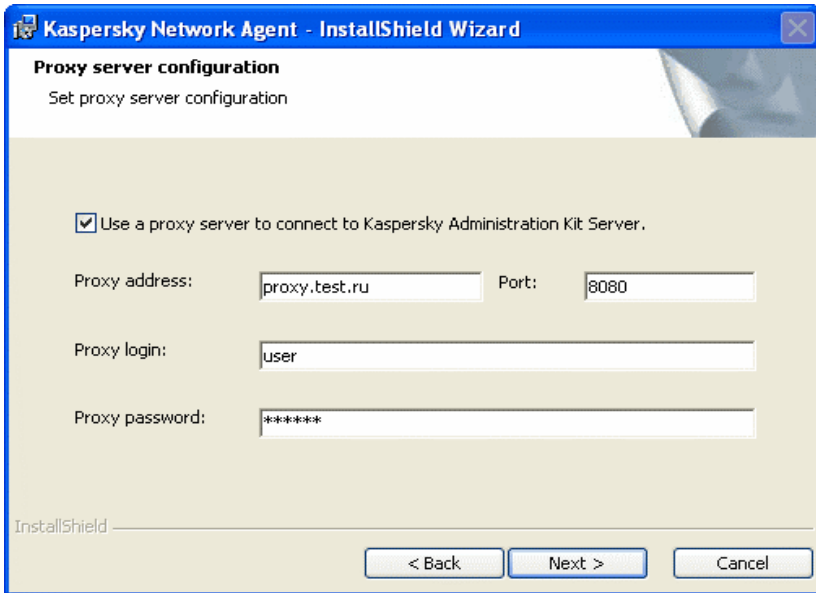


Figure 51. Configuring the connection settings via a proxy server

6. After this, determine which folder of the **Network** group the computer must be added to after it is detected by the Administration Server during the Windows network polling. Select one of the following options: (see Figure 52):
 - **Default group name** - the computer will be added to the folder that corresponds to its position in the Windows network: domain or the workgroup (this is the default option).
 - **Define group name** - the computer will be added to the folder specified in the **Group name** field. If you select this option, enter the folder name. If such folder does not exist in the **Network** group, it will be created (you can specify the name of any of the folders existing in the **Network** group).



Figure 52. Selecting the group in the **Network** folder to store the computers

7. During the next stage (see Figure 53) you have to specify the method you would like to use to receive the certificate of the Administration Server's to which the Network Agent will connect. Select one of the following options:
 - **Default certificate** - the Administration Server's certificate will be received when the Network Agent connects to it for the first time (this is the default options);
 - **Select certificate file** - authentication at the Administration Server will be performed based on the certificate specified by the administrator. If you select this option, specify the Administration Server's certificate file to be used.

The certificate file has extension **.cer** and is located on the Administration Server in the **Cert** folder in the Kaspersky Administration Kit installation folder.

You can copy the certificate file to the shared folder or onto a disk and use a copy of the file to install the Network Agent.

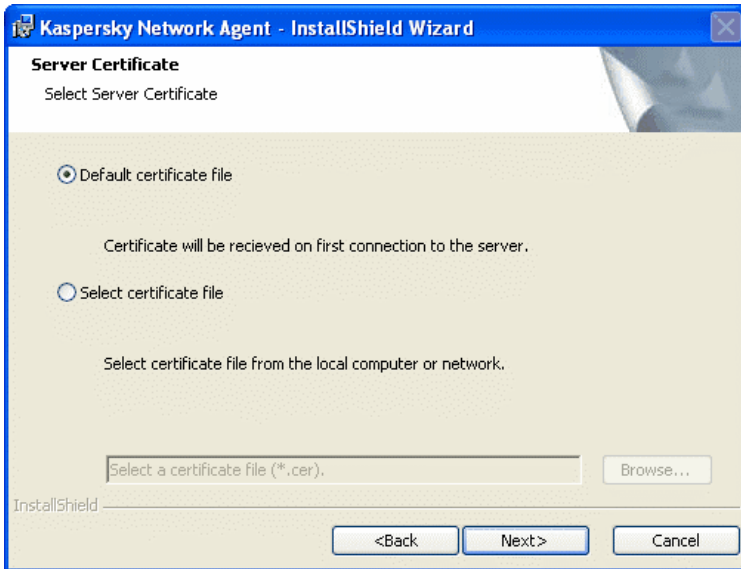


Figure 53. Selecting the method to be used to receive the Administration Server's certificate

8. In the final wizard window (see Figure 54) you will be offered to run the Network Agent immediately after the wizard is complete. If you would like to run it later, uncheck the **Launch Network Agent** box checked by default.

If you are planning to use the hard drive of the computer on which the Network Agent is installed in order to create a disk image and deploy it on other computers, the **Launch Network Agent** box must be unchecked.

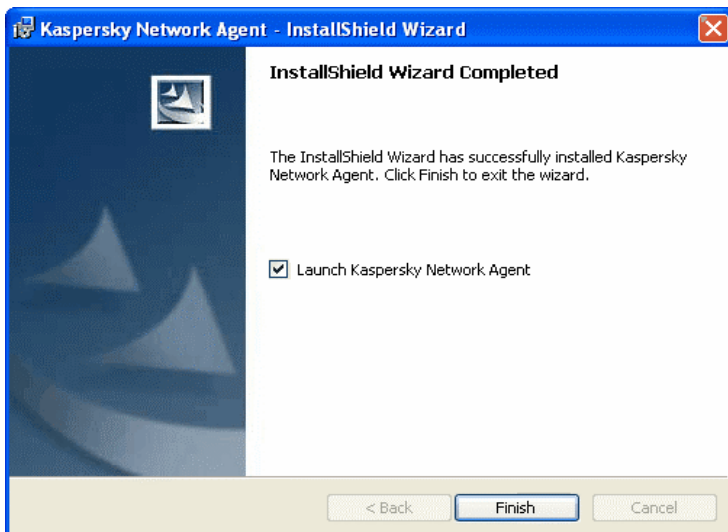


Figure 54. Configuring the launch of the Network Agent

After the wizard is complete, the Network Agent will be installed on your computer.

You can review the properties of the **Kaspersky Network Agent** service, start, stop or monitor it using the standard Windows administration tools - **Computer Management** → **Services**.

A plugin for cooperation with Cisco Network Admission Control (NAC) is always installed to a host together with an Administration Agent. The plugin is invoked if the Cisco Trust Agent application is installed.

4.3.2. Local installation of the application administration plugin

In order to install the application administration plugin,

on the computer on which the Administration Console is installed, run executable file **klcginst.exe**, located on the application's distribution CD. This file is included into all applications that can be administered via Kaspersky Administration Kit. The installation is facilitated by a wizard and does not require any configuration. It will offer you to configure the installation settings and start it.

The file of the administration plugin for the Network Agent **klcfiginst.exe** is located in the **NetAgent** folder of the distribution package of Kaspersky Administration Kit

4.3.3. Installing applications in non-interactive mode

In order to install an application in non-interactive mode:

1. Create the required installation package (see section 4.1.1xx) if the installation package for the application you would like to install has not been created.

Installation packages will be saved in some shared folder under the Administration Server **Packages** system directory when the Administration Server is being installed. A subfolder will correspond to each installation package.

2. Configure installation package settings as required.
3. Install application using one of the methods below:

Copy the entire folder corresponding to the desired installation package from the Administration Server to the client. Open the copied folder on the client and start the executable (file with the **.exe** extension) using the **/s** switch.

Access the shared folder for the desired installation package on the Administration Server from the client. Then start the executable with the **/s** switch.

4. Run executable file **setup.exe** with modifier **/s** included into the distribution package of the application being installed, on the computer onto which you plan to install the application using non-interactive mode.

Installation packages are stored on the Administration Server in the shared folder specified during the Administration Server installation stage, in service folder **Packages**.

When installing Kaspersky Administration Kit non-interactively, an answer file may be used. This file contains all the application install parameters and enables the application to be installed more than once with the same parameters.

To generate a Kaspersky Administration Kit answer file:

1. Use the command line to go to the folder containing a Kaspersky Administration Kit distribution and run the executable with switches **/r** and **/f1"<file path>\setup.iss"**³ (for example, **setup.exe /r /f1"C:\setup.iss"**).
 - This will start the application installation wizard on the host computer.
2. Follow the prompts offered by the wizard to configure application installation settings. For example, Administration Server or Console only may be selected for installation.

Once the installation is complete, the selected version of Kaspersky Administration Kit will have been installed on the host computer, and an answer file will have been generated and placed in the specified directory. The resulting answer file should be copied into the relevant installation package folder on the Administration Server. This will cause Kaspersky Administration Kit to install non-interactively using one of the methods above with the configuration specified in the answer file.

An answer file may be used to update Kaspersky Administration Kit non-interactively. However, it can only be used to update the application version that had been utilized to generate the file.

³ The complete path to the answer file must be specified.

APPENDIX A. GLOSSARY

This Guide uses some specific terms related to anti-virus protection. Glossary is a list of definitions of these terms. The glossary entries are arranged in alphabetical order to facilitate using the glossary.

A

Available updates – Service Packs that contain urgent updates accumulated over time and latest changes in the application architecture.

Administration group – Computers grouped in accordance with their functional and installed Kaspersky Lab applications. Grouping significantly facilitates the management process and allows the administrator to manage all computers as a single entity. A group might include other groups. Group policies and group tasks can be created for each application of installed on group members.

Administration Console– A Kaspersky Administration Kit component that provides user interface for the administrative services of the Administration Server and Network Agent.

Anti-virus database – A database created by Kaspersky Lab specialists that contains detailed definitions of all currently existing viruses and methods for their detection and disinfection. Anti-virus applications use the database to successfully detect and disinfect viruses. The anti-virus database available on the Kaspersky Lab websites is regularly updated as new virus threats appear. Registered users of Kaspersky Lab applications have access to database updates. To keep your computer constantly protected from viruses, we strongly recommend that you download updates on a regular basis.

Administrator workstation – A computer where the Administration Console of Kaspersky Administration Kit is installed. Using the Console, the administrator can build and manage the anti-virus protection system based on Kaspersky Lab applications.

Anti-virus protection status – Current status of anti-virus protection that characterizes the security level for your computer.

Administration Server – A Kaspersky Administration Kit component that centrally stores information about Kaspersky Lab applications installed on clients and manages these applications.

Administration Server certificate – A certificate used to authenticate the Administration Server upon connection of the Administration Console to the server and data transmission between the server and clients. The Administration Server certificate is created during the installation of the

Administration Server. It is located in the **Cert** folder of the installation folder.

B

Block object – Prevent external applications from accessing an object. The blocked object cannot be read, executed, modified, or deleted.

Backing up – copying data of the Administration server for storage and subsequent restoration performed by the backup utility. The utility allows to save:

Administration Server database that stores policies, tasks, application settings, and events logged on the Administration Server

Information about the logical networks and client configurations

Installation files for the remote installation of applications (contents of the Packages, Uninstall, Updates folders)

Administration Server certificate

Backup folder – A directory that contains backups of deleted and disinfected objects.

Backup license key – a license key installed for a Kaspersky Lab's application, but not activated. Depending on the settings, activation of the key can be performed automatically upon the expiration of the current key or manually.

Backup storage – A folder that contains the backup copies of Administration Server data created by the backup utility.

C

Console (management) plug-in – A special component that provides an interface for remotely managing an application through the Administration Console. The plug-ins are specific to each application and are included in all Kaspersky Lab applications that can be managed through Kaspersky Administration Kit.

Centrally managing an application – Managing an application through Kaspersky Administration Kit.

Client, Administration Server (or client computer) – a computer, a server, or a workstation with the installed Network Agent and managed Kaspersky Lab applications.

Current license key – a license key installed and currently used to work with a Kaspersky Lab's application. This key determines the license period and the licensing policy regarding to the product.

D

Disinfection – A method of treating infected objects. Disinfection implies partial or full recovery of data or results in a decision that these files cannot be disinfected. Objects are disinfected using the anti-virus database. If disinfection is the first action to be applied to an object, i. e.

the first action after detection of a suspicious object, the program creates a backup of this file. If some data are lost during disinfection, you can use the backup to recover this object.

Deleting an object – A method of handling an object. To delete an object is to remove it physically from a computer. This method is recommended for treating infected objects. If deleting is the first action applied to an object, it is necessary to create a backup of this object before deleting it. You can use the backup to restore the original object.

E

Exclusions – User-defined settings that exclude certain objects from scans. You can customize the exclusion rules for *real-time protection* and *on-demand scans*. Thus, you can disable scanning of archives during a full scan or exclude files from scans by their masks.

E-mail databases – Databases that contain e-mail messages stored on your computer. Every incoming/outgoing message is saved in the database after you receive/send it. Such databases are scanned in the on-demand scanning mode.

F

Forced installation – a method of remote installation of Kaspersky Lab's applications that allows to perform remote installation on specific client computers of the logical network. In order to ensure successful execution of a forced installation task the account used to run the task must have the right for remote launch of the applications on the client computers of the logical network. This method is recommended for installation of applications onto computers running Microsoft Windows NT/2000/2003/XP that support such feature or onto computers running Microsoft Windows 98/Me on which the Network Agent is installed.

G

Global task – A task defined for and running on a number of clients from different administration groups.

Group Task – A task defined for and running on all clients in a group.

Group policy – A set of application settings in an administration group managed through Kaspersky Administration Kit. Group policies can be different for each group. Group policies are specific to individual applications. The policy involves configuration of all parameters of applications.

I

IChecker technology – A technology that excludes the objects from future scans that remained unmodified since the last scan. The IChecker technology was implemented by using the object checksum database.

IStreams technology – A technology that excludes the files stored on NTFS-formatted disks that remained unmodified since the last scan. The IStreams technology was implemented by using a method of storing file checksums in the additional NTFS streams.

Infected object – An object containing a virus. We recommend that you abandon working on these objects because they can infect your computer.

Installation package – A package of files used to install Kaspersky Lab applications on remote hosts on a logical network. Installation packages are based on a special **.kpd** file included in the application distribution kit, which contains a minimum set of parameters that provide the basic functionality of the application immediately after the installation. The values of the parameters are default settings of the applications.

Installation using the startup scenario – a method of remote installation of Kaspersky Lab's applications that allows to assign a remote installation task to a specific account of a user (or several users). When a user is registered with a domain, an attempt will be made to install the application on the client computer from which the user has registered. This method is recommended for installation of Kaspersky Lab's applications onto computers running Microsoft Windows 98/Me.

K

Kaspersky Lab update servers – A list of http and ftp Kaspersky Lab websites where you can copy updates to your computer from.

Kaspersky Administration Kit – An application for centralized performance of key administrative tasks. It gives you complete control over the enterprise anti-virus policy based on Kaspersky Lab applications.

L

License key – A file with the **.key** extension that serves as your personal "key". This file is required for correct operation of Kaspersky Lab applications. The license key is included in the distribution kit if you purchased your copy of the application from Kaspersky Lab distributors. If you purchased the application online, the license key is sent to you via e-mail. Without the license key, Kaspersky Anti-Virus DOES NOT WORK.

Logical network operator – A user that monitors the system of anti-virus protection managed by Kaspersky Administration Kit.

Local management – Management of an application through a local interface.

Local task – A task created for and running on a single client.

License period – A period during which you have the right to take advantage of the full functionality of Kaspersky Anti-Virus. As a rule, the

license period defined by the license key is one year from the date of purchase. After your license expires, the application will operate but you will not be able to update the *anti-virus database*.

Local network administrator – A user who installs, configures, and maintains Kaspersky Administration Kit and remotely manages Kaspersky Lab applications installed on the logical network computers.

M

Maximum protection – A protection level that ensures comprehensive protection but slightly decreases performance characteristics.

Maximum speed – A protection level that has a maximum operation speed but a lower security level.

N

Network Agent – A Kaspersky Administration Kit component that provides communication between the Administration Server and Kaspersky Lab applications installed on specific network nodes (workstations or servers). This component is common to all Windows applications included in Kaspersky Lab Business Optimal and Corporate Suite. Separate versions of Administration Agent exist for Kaspersky Lab Novell and UNIX applications.

O

OLE-object – An object linked or embedded into other files by using OLE technology.

On-demand full scan – An administrator-defined mode that scans all files on your computer for viruses and disinfects/deletes infected objects upon their detection.

P

Policy – see **Group policy**

Push installation – A remote installation method that allows you to install Kaspersky Lab software on specified computers on your logical network. In order to successfully perform the task using a push installation, the account used to launch this task must have rights to run applications on remote clients. This method is recommended for computers running MS Windows NT/2000/2003/XP, which support this feature, or for computers that are running MS Windows 98/Me and have an installed Network Agent.

Q

Quarantining – A method of handling a *suspicious* object. Access to this object is blocked and the file is moved to the quarantine for further processing.

Quarantine – A special storage that isolates infected and suspicious objects.

R

Real-time protection – A scanning mode in which an anti-virus application is memory resident. In the real-time protection mode, the application scans all objects when you open them for reading, writing, or executing. Before enabling access to an object, Kaspersky Anti-Virus scans it for viruses and, if a virus is detected, blocks access to the object, disinfects it or deletes it (depending on user-defined settings).

Recommended level – The level of antivirus protection with default settings recommended by Kaspersky Lab experts which ensures the optimal protection of your computer. This level is set by default.

Remote installation– Installation of Kaspersky Lab applications using the services provided by Kaspersky Administration Kit.

Restoring – Restoring Administration Server data using a backup utility. The information for restoring is available in the backup storage. The utility allows you to restore:

Administration Server database that stores policies, tasks, application settings, and events logged on the Administration Server

Information about the logical networks and client configurations

Installation files for the remote installation of applications (contents of the Packages, Uninstall, Updates folders)

Administration Server certificate

S

Script-based installation – An installation method that relates the remote installation task with a specified user account (several accounts). When the specified user logs onto the domain, the application will be installed on the client where this user has logged on. This method is recommended for use with computers running MS Windows 95/98/Me

Settings, task – Application settings specific for each type of task.

Settings, applications – Application settings specific for all types of tasks performed by this application.

Severity level – A parameter that classifies an event recorded during Kaspersky Anti-Virus performance. There are four severity levels:

- **Critical**
- **Error**
- **Warning**
- **Info**

Events of the same kind can be of different severity levels, depending on a specific situation.

Startup objects – A set of programs that are necessary for launching and smooth operation of the operating system and other software installed on your computer. Your operating system launches these objects during each startup. Some viruses attempt to infect the startup objects and can cause a startup failure.

Suspicious object – An object that contains either a modified code of a well-known virus or a code reminiscent of a virus yet unknown to Kaspersky Lab specialists.

Scan files by format – In this scanning mode, the program analyzes the contents of a file, namely, the format identifier in the file header.

Scan files by extension – In the scanning mode, the program takes into account the scanned file extension.

T

Task – An action that has a name performed by a Kaspersky Lab application.

Third party application – An anti-virus application by a third-party vendor or a Kaspersky Lab's application not supporting administration via Kaspersky Administration Kit.

U

Unknown virus – A new virus that is not recorded in the *anti-virus database*. As a rule, Kaspersky Anti-Virus detects unknown viruses using an *heuristic code analyzer* and objects containing these viruses are identified as *suspicious*.

Updating – A function of Kaspersky Anti-Virus that updates/adds new files (anti-virus database or program modules) retrieved from Kaspersky Lab update servers.

Updating agents - computers that act as intermediate centers for distributing updates and installation packages within the administration groups.

V

Virtual drives (RAM drives) – A part of RAM emulating a normal physical disk of a personal computer.

Virus activity threshold – number of viruses detected for a specified time interval. When this number is exceeded, the situation is regarded as a **Virus outbreak** (virus attack). This parameter is important for defining virus epidemics because the administration can respond in a timely fashion to new threats and take preventive measures to protect his/her network.

APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, email systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

B.1. Other Kaspersky Lab Products

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, notifications about the current status of virus activity, and fresh news. The program reads the list of available news feeds and their content from the Kaspersky Lab news server at specified intervals.

News Agent enables users to;

- See the current virus forecast .in the system tray
- Subscribe to and unsubscribe from news feeds
- Retrieve news from each selected feed at the specified interval and receive notifications about fresh news
- Review news on the selected feeds
- Review the list of feeds and their status
- Open full article text in your browser

News Agent is a stand-alone Microsoft Windows application that can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

This program is a free service provided to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. This way, users receive quick responses to questions regarding potential infections on their computers. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky® OnLine Scanner Pro

The program is a subscription service available to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer and disinfects dangerous files. Kaspersky OnLine Scanner Pro runs directly from your browser. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks, including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used, as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, folders, or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

Controls modifications within the file system. The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.

Monitors processes in random-access memory. Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.

Monitors changes in OS registry due to internal system registry control.

Hidden Processes Monitor helps protect from malicious code concealed in the operating system using rootkit technologies.

Heuristic Analyzer. When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.

Performs system restore after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 is an integrated solution for protection of personal computers against the major information- threats (viruses, hackers, spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.

Real-time anti-virus scanning of Internet traffic transferred via HTTP.

File system protection: anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.

Proactive protection: the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks such activity. *Privacy Control* module keeps your confidential information secure from unauthorized access and transmission. *Parental Control* is a Kaspersky Internet Security component that monitors user access to the Internet.

Kaspersky Internet Security 7.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical network attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth Mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch to Stealth Mode, the system blocks all network activity except for a few transactions allowed in user-defined rules.

The program employs an all-inclusive approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites)
- Inspection of phrases in message body
- Analysis of message text using a learning algorithm
- Recognition of spam sent in image files

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile provides antivirus protection for mobile devices running Symbian OS and Microsoft Windows Mobile. The program provides comprehensive virus scanning, including:

- **On-demand scans** of the mobile device's onboard memory, memory cards, an individual folder, or a specific file; if an infected file is detected, it is moved to Quarantine or deleted
- **Real-time scanning** – all incoming and outgoing files are automatically scanned, as well as files when attempts are made to access them
- **Protection from text message spam**

Kaspersky Anti-Virus for File Servers

This software package provides reliable protection for file systems on servers running Microsoft Windows, Novell NetWare, Linux and Samba from all types of malware. The suite includes the following Kaspersky Lab applications:

- [Kaspersky Administration Kit](#).
- [Kaspersky Anti-Virus for Windows Server](#).
- [Kaspersky Anti-Virus for Linux File Server](#).
- [Kaspersky Anti-Virus for Novell Netware](#).
- [Kaspersky Anti-Virus for Samba Server](#).

Features and functionality:

- *Protects server file systems in real time:* All server files are scanned when opened or saved on the server
- *Prevents virus outbreaks;*
- *On-demand scans* of the entire file system or individual files and folders;
- *Use of optimization technologies* when scanning objects in the server file system;
- *System rollback after virus attacks;*

- *Scalability of the software package* within the scope of system resources available;
- *Monitoring of the system load balance*;
- *Creating a list of trusted processes* whose activity on the server is not subject to control by the software package;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Saving backup copies of infected and deleted objects* in case you need to restore them;
- *Quarantining suspicious objects*;
- *Send notifications on events* in program operation to the system administrator;
- *Log detailed reports*;
- *Automatically update* program databases.

Kaspersky Open Space Security

Kaspersky Open Space Security is a software package with a new approach to security for today's corporate networks of any size, providing centralized protection information systems and support for remote offices and mobile users.

The suite includes four programs:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifics on each program are given below.

Kaspersky Workspace Security is a program for centralized protection of workstations inside and outside of corporate networks from all of today's Internet threats (viruses, spyware, hacker attacks, and spam).

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam*;
- *Proactive Defense from new malicious programs whose signatures are not yet added to the database*;
- *Personal Firewall with intrusion detection system and network attack warnings*;

- *Rollback for malicious system modifications;*
- *Protection from phishing attacks and junk mail;*
- *Dynamic resource redistribution during complete system scans;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Scanning of e-mail and Internet traffic in real time;*
- *Blocking of popup windows and banner ads when on the Internet;*
- *Secure operation in any type of network, including Wi-Fi;*
- *Rescue disk creation tools that enable you to restore your system after a virus outbreak;*
- *An extensive reporting system on protection status;*
- *Automatic database updates;*
- *Full support for 64-bit operating systems;*
- *Optimization of program performance on laptops (Intel® Centrino® Duo technology);*
- *Remote disinfection capability (Intel® Active Management, Intel® vPro™).*

Kaspersky Business Space Security provides optimal protection of your company's information resources from today's Internet threats. Kaspersky Business Space Security protects workstations and file servers from all types of viruses, Trojans, and worms, prevents virus outbreaks, and secures information while providing instant access to network resources for users.

Features and functionality:

- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Protection of workstations and file servers from all types of Internet threats;*
- *iSwift technology to avoid rescanning files within the network;*
- *Distribution of load among server processors;*
- *Quarantining suspicious objects from workstations;*
- *Rollback for malicious system modifications;*
- *scalability of the software package within the scope of system resources available;*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database;*

- *Scanning of e-mail and Internet traffic in real time;*
- *Personal Firewall with intrusion detection system and network attack warnings;*
- *Protection while using Wi-Fi networks;*
- *Self-Defense from malicious programs;*
- *Quarantining suspicious objects;*
- *Automatic database updates.*

Kaspersky Enterprise Space Security

This program includes components for protecting linked workstations and servers from all today's Internet threats. It deletes viruses from e-mail, keeping information safe while providing secure access to network resources for users.

Features and functionality:

- *Protection of workstations and file servers from viruses, Trojans, and worms;*
- *Protection of Sendmail, Qmail, Postfix and Exim mail servers;*
- *Scanning of all e-mails on Microsoft Exchange Server, including shared folders;*
- *Processing of e-mails, databases, and other objects for Lotus Domino servers;*
- *Protection from phishing attacks and junk mail;*
- *preventing mass mailings and virus outbreaks;*
- *scalability of the software package within the scope of system resources available ;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco ® NAC (Network Admission Control);*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation while using Wi-Fi networks;*
- *Scans Internet traffic in real time;*
- *Rollback for malicious system modifications;*
- *Dynamic resource redistribution during complete system scans;*
- *Quarantining suspicious objects ;*

- *An extensive reporting system on protection system status;*
- *automatic database updates.*

Kaspersky Total Space Security

This solution monitors all inbound and outbound data streams (e-mail, Internet, and all network interactions). It includes components for protecting workstations and mobile devices, keeps information safe while providing secure access for users to the company's information resources and the Internet, and ensures secure e-mail communications.

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam on all levels of the corporate network, from workstations to Internet gateways;*
- *Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;*
- *Protection of mail servers and linked servers;*
- *Scans Internet traffic (HTTP/FTP) entering the local area network in real time;*
- *scalability of the software package within the scope of system resources available ;*
- *Blocking access from infected workstations;*
- *Prevents virus outbreaks;*
- *Centralized reporting on protection status;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco® NAC (Network Admission Control);*
- *Support for hardware proxy servers;*
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *iSwift technology to avoid rescanning files within the network ;*
- *Dynamic resource redistribution during complete system scans;*
- *Personal Firewall with intrusion detection system and network attack warnings ;*
- *Secure operation for users on any type of network, including Wi-Fi;*

- *Protection from phishing attacks and junk mail;*
- *Remote disinfection capability (Intel® Active Management, Intel® vPro™);*
- *Rollback for malicious system modifications;*
- *Self-Defense from malicious programs;*
- *full support for 64-bit operating systems;*
- *automatic database updates.*

Kaspersky Security for Mail Servers

This program is for protecting mail servers and linked servers from malicious programs and spam. The program includes application for protecting all standard mail servers (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim) and also enables you to configure a dedicated e-mail gateway. The solution includes:

- [Kaspersky Administration Kit.](#)
- [Kaspersky Mail Gateway.](#)
- [Kaspersky Anti-Virus for Lotus Notes/Domino.](#)
- [Kaspersky Anti-Virus for Microsoft Exchange.](#)
- [Kaspersky Anti-Virus for Linux Mail Server.](#)

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Junk mail filtering;*
- *Scans incoming and outgoing e-mails and attachments;*
- *Scans all e-mails on Microsoft Exchange Server for viruses, including shared folders;*
- *Processes e-mails, databases, and other objects for Lotus Notes/Domino servers;*
- *Filters e-mails by attachment type;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system for the program;*
- *Prevents virus outbreaks;*
- *Monitors protection system status using notifications;*
- *Reporting system for program operation;*

- scalability of the software package within the scope of system resources available ;
- *automatic database updates.*

Kaspersky Security for Internet Gateways

This program provides secure access to the Internet for all an organization's employees, automatically deleting malware and riskware from the data incoming on HTTP/FTP. The solution includes:

- [Kaspersky Administration Kit.](#)
- [Kaspersky Anti-Virus for Proxy Server.](#)
- [Kaspersky Anti-Virus for Microsoft ISA Server.](#)
- [Kaspersky Anti-Virus for Check Point FireWall-1.](#)

Its features include:

- *Reliable protection from malicious or potentially dangerous programs;*
- *Scans Internet traffic (HTTP/FTP) in real time;*
- *Filters Internet traffic using a trusted server list, object types, and user groups;*
- *Quarantines suspicious objects;*
- *Easy-to-use administration system;*
- *Reporting system for program operation;*
- *Support for hardware proxy servers;*
- Scalability of the software package within the scope of system resources available ;
- *Automatic database updates.*

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail.

The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database, adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper provides high-speed scanning of traffic on servers running Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

The program is a plug-in and scans for viruses and processes inbound and outbound e-mail traffic in real time.

B.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: info@kaspersky.com

APPENDIX C. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS (“SOFTWARE”) PRODUCED BY KASPERSKY LAB (“KASPERSKY LAB”).

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD’S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD’S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER’S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

1. *License Grant.* Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes.

1.1 *Use.* The number of computers that User may protect by the Software is specified in the License Key File and indicated in the "Service" window. The Software may not be used to protect any networks with more than this number of file servers.

1.1.1 The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab's update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.1.8 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 Removal of Potentially Harmful Products. You acknowledge and agree that, in addition to detecting harmful and malicious software, the Product may also identify, remove and/or disable potentially harmful products, including those that are regarded or classified as Adware, Riskware, Pornware etc.

2. Support.

- (i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of purchasing on:
 - (a) payment of its then current support charge, and;
 - (b) Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.
 - (c) Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.
- (ii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.
- (iii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.
- (iv) "Support Services" means:
 - (a) Hourly updates of the anti-virus database;
 - (b) Free software updates, including version upgrades;
 - (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
 - (d) Virus detection and disinfection updates in 24-hours period.

- (v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *Ownership Rights.* The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality.* You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavors to maintain the security of the activation code.

5. *Limited Warranty.*

- (i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.
- (ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.
- (iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) Kaspersky Lab does not warrant that this Software provides protection after expiring date (see section.2 (i))
- (v) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as

may be reasonably necessary to assist the Supplier in resolving the defective item.

- (vi) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.
- (vii) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability.*

- (i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.
- (ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):
 - (a) Loss of revenue;
 - (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
 - (c) Loss of the use of money;
 - (d) Loss of anticipated savings;
 - (e) Loss of business;
 - (f) Loss of opportunity;
 - (g) Loss of goodwill;
 - (h) Loss of reputation;
 - (i) Loss of, damage to or corruption of data, or:

- (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.

When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).