

KASPERSKY LAB

---

Kaspersky<sup>®</sup> Administration Kit  
version 6.0

Reference Book

KASPERSKY® ADMINISTRATION KIT  
VERSION 6.0

---

# Reference Book

© Kaspersky Lab Ltd.  
Visit our website: <http://www.kaspersky.com/>

Revision date: February, 2006

# Contents

|  |    |
|--|----|
| CHAPTER 1. KASPERSKY® ADMINISTRATION KIT.....  | 8  |
| 1.1. The purpose of this document .....  | 9  |
| 1.2. Conventions used in this book .....   | 10 |
| CHAPTER 2. MANAGING THE LOGICAL NETWORK .....  | 11 |
| 2.1. Starting the Administration Console and connecting to the Administration<br>Server .....                              | 11 |
| 2.1.1. Starting the Administration Console.....  | 11 |
| 2.1.2. Connecting to the Administration Server .....   | 11 |
| 2.1.3. Disconnecting from the Administration Server .....  | 15 |
| 2.1.4. Switching between servers.....  | 15 |
| 2.1.5. Adding a server to the console tree .....   | 15 |
| 2.1.6. Removing a server from the console tree.....  | 16 |
| 2.2. Granting rights .....   | 16 |
| 2.2.1. Granting rights to use the Administration Servers .....   | 16 |
| 2.2.2. Granting rights to groups .....   | 18 |
| 2.3. Viewing information about networks and IP subnetworks .....   | 20 |
| 2.3.1. Viewing information about the computer network .....  | 20 |
| 2.3.2. Method for displaying the computer network.....   | 20 |
| 2.3.3. Creating an IP subnetwork .....   | 21 |
| 2.3.4. Viewing and modifying the IP subnetwork settings .....  | 22 |
| 2.3.5. Viewing and Modifying Active Directory Group Parameters .....   | 25 |
| 2.4. Quick Start Wizard.....   | 26 |
| 2.4.1. Using the Quick Start Wizard .....  | 26 |
| 2.5. Creating, viewing and configuring a logical network .....   | 32 |
| 2.5.1. Viewing information about groups.....   | 32 |
| 2.5.2. Viewing group properties, and configuring interactions between client<br>computers and Administration Servers ..... | 33 |
| 2.5.3. Viewing information about the client computer .....   | 37 |
| 2.5.4. Viewing the logical network of a slave Administration Server .....  | 41 |
| 2.6. Groups .....  | 42 |
| 2.6.1. Adding a group .....  | 42 |

|   |    |
|---|----|
| 2.6.2. Configuring group settings .....   | 43 |
| 2.6.3. Configuring automatic installation of software on new computers in the group .....                               | 50 |
| 2.6.4. Moving groups .....  | 50 |
| 2.6.5. Renaming groups .....  | 50 |
| 2.6.6. Deleting a group.....  | 51 |
| 2.7. Client computers.....  | 51 |
| 2.7.1. Adding computers to the logical network.....   | 51 |
| 2.7.2. Automatically adding new computers to a group.....   | 52 |
| 2.7.3. Moving a client computer to a different logical network. Administration Server change task.....                  | 53 |
| 2.7.4. Manually connecting the client computer to the Administration Server. The <i>klmover.exe</i> utility .....       | 57 |
| 2.7.5. Verifying manual connection of the client computer to Administration Server The <i>klhagchk.exe</i> utility..... | 58 |
| 2.8. Slave Administration Servers.....  | 59 |
| 2.8.1. Adding a new slave Administration Server.....  | 59 |
| 2.8.2. Configuring the connection of the slave server to the main server.....   | 61 |
| CHAPTER 3. REMOTE APPLICATION MANAGEMENT .....  | 63 |
| 3.1. Configuring application settings .....   | 63 |
| 3.1.1. Managing policies .....  | 63 |
| 3.1.1.1. Creating a policy .....  | 63 |
| 3.1.1.2. Viewing and configuring policy settings .....  | 66 |
| 3.1.1.3. Displaying Inherited Policy in Nested Group Result Panel .....   | 78 |
| 3.1.1.4. Activating a policy .....  | 79 |
| 3.1.1.5. Activating a policy based on an event.....   | 79 |
| 3.1.1.6. Policy for mobile user.....  | 80 |
| 3.1.1.7. Deleting a policy.....   | 80 |
| 3.1.1.8. Copying a policy.....  | 80 |
| 3.1.1.9. Configuring the Network Agent's policy .....   | 81 |
| 3.1.1.10. Configuring the settings of the Administration Server policy.....   | 85 |
| 3.1.1.11. Exporting policies .....  | 90 |
| 3.1.1.12. Importing policies .....  | 90 |
| 3.1.2. Viewing application settings .....   | 91 |
| 3.1.2.1. Viewing application settings .....   | 91 |
| 3.1.2.2. Administration Server settings.....  | 95 |

---

|  |     |
|--|-----|
| 3.1.2.3. Configuring Network Agent .....   | 110 |
| 3.2. Managing applications' operation .....  | 112 |
| 3.2.1. Creating a group task .....   | 112 |
| 3.2.2. Creating a global task .....  | 122 |
| 3.2.3. Creating a local task .....   | 123 |
| 3.2.4. Viewing and changing task settings .....  | 124 |
| 3.2.5. Displaying Inherited Group Task in Nested Group Result Pane .....                             | 131 |
| 3.2.6. Automatic operating system loading on the client computers before the<br>task execution ..... | 132 |
| 3.2.7. Turning off the computer after the task completion .....                                      | 132 |
| 3.2.8. Restricting time for the task execution .....   | 133 |
| 3.2.9. Canceling scheduled task launch .....   | 133 |
| 3.2.10. Creating application start / stop task .....   | 133 |
| 3.2.11. Exporting and importing tasks .....  | 135 |
| 3.2.12. Importing a task .....   | 135 |
| 3.2.13. Starting and stopping tasks manually .....   | 135 |
| 3.2.14. Pausing/resuming tasks manually .....  | 136 |
| 3.2.15. Monitoring task execution .....  | 136 |
| 3.2.16. Viewing results of the task execution stored on the Administration<br>Server .....           | 137 |
| 3.2.17. Configuring the event filter for a group task .....  | 138 |
| 3.2.18. Configuring event filter for a selected computer .....                                       | 141 |
| 3.2.19. Removing a filter .....  | 143 |
| <br>   |     |
| CHAPTER 4. UPDATING THE ANTI-VIRUS DATABASE AND PROGRAM<br>MODULES .....                             | 144 |
| 4.1. Downloading updates by the Administration Server .....  | 144 |
| 4.1.1. Creating task for receiving updates by the Administration Server .....                        | 144 |
| 4.1.2. Configuring the update task .....   | 147 |
| 4.1.3. Viewing the list of updates .....   | 149 |
| 4.1.4. Viewing properties of the downloaded updates .....  | 149 |
| 4.2. Automatic distribution of updates .....   | 151 |
| 4.2.1. Automatic distribution of updates on the client computers .....                               | 151 |
| 4.2.2. Automatic distribution of update to the slave servers .....                                   | 151 |
| 4.2.3. Creating the list of the updating agents and configuring the agents .....                     | 151 |
| <br>   |     |
| CHAPTER 5. MAINTENANCE .....   | 154 |

|   |     |
|---|-----|
| 5.1. Renewing your license .....  | 154 |
| 5.1.1. Viewing information about installed license keys .....                                     | 154 |
| 5.1.2. Viewing license key details.....   | 154 |
| 5.1.3. Installing a license key.....  | 156 |
| 5.1.4. Running the License key installation task creation wizard .....                            | 157 |
| 5.1.5. Creating and viewing license keys report .....   | 158 |
| 5.2. Quarantine and backup storage .....  | 159 |
| 5.2.1. Viewing properties of quarantined or backed-up objects .....                               | 159 |
| 5.2.2. Removing objects from the quarantine or backup storage .....                               | 160 |
| 5.2.3. Restoring objects from the quarantine or backup storage .....                              | 160 |
| 5.2.4. Scanning the quarantine folder on the client computer.....                                 | 161 |
| 5.3. Event logs. Event queries .....  | 161 |
| 5.3.1. Viewing Kaspersky Administration Kit event log stored on the<br>Administration Server..... | 161 |
| 5.3.2. Creating event queries .....   | 162 |
| 5.3.3. Customizing event queries.....   | 163 |
| 5.3.4. Saving information about events to a file.....   | 167 |
| 5.3.5. Deleting events .....  | 167 |
| 5.4. Reports .....  | 167 |
| 5.4.1. Creating a report template.....  | 167 |
| 5.4.2. Viewing and editing report templates.....  | 170 |
| 5.4.3. Generating and viewing reports .....   | 175 |
| 5.4.4. Generating summary reports on slave Administration Servers .....                           | 177 |
| 5.4.5. Restricting the number of records included in the report.....                              | 178 |
| 5.5. Monitoring Antivirus Protection Status Using System Registry Data .....                      | 178 |
| 5.6. Finding computers .....  | 180 |
| 5.6.1. Finding computers .....  | 180 |
| 5.6.2. Saving computer search results in a text file .....  | 185 |
| 5.7. Computers selections.....  | 186 |
| 5.7.1. Configuring a computer query.....  | 186 |
| 5.7.2. Configuring a computer query.....  | 186 |
| 5.8. Tracking virus outbreaks .....   | 192 |
| 5.8.1. Enabling virus attack detection mechanism .....  | 192 |
| 5.8.2. Changing the application policy when a Virus attack event is registered .....              | 193 |
| 5.9. Backup copying and restoration of Administration Server data.....                            | 194 |
| 5.9.1. Backup copying of Administration Server data.....  | 194 |

---

|   |     |
|---|-----|
| 5.9.2. Restoring the Administration Server data from a backup copy.....   | 194 |
| 5.9.3. Backup data copying task .....   | 194 |
| 5.9.3.1. Creating a backup data copying task .....  | 194 |
| 5.9.3.2. Configuring the Administration Server data backup copying task .....                                   | 197 |
| 5.9.4. Backup data copying utility .....  | 198 |
| 5.9.4.1. Creating a backup copy of the Administration Server data manually.<br>The <i>kbackup</i> utility ..... | 198 |
| 5.9.4.2. Moving the Administration Server to a different computer .....   | 200 |
| 5.9.4.3. Moving the Administration Server database to a different computer .....                                | 201 |
| 5.10. Configuring Integration with Cisco Network Admission Control (NAC).....                                   | 202 |
| APPENDIX A. HOW TO CONTACT TECHNICAL SUPPORT SERVICE.....   | 203 |
| APPENDIX B. GLOSSARY .....  | 205 |
| APPENDIX C. KASPERSKY LAB.....  | 212 |
| C.1. Other Kaspersky Lab Products .....   | 213 |
| C.2. Contact Us .....   | 223 |
| APPENDIX D. LICENSE AGREEMENT .....   | 224 |

---

# CHAPTER 1. KASPERSKY®

## ADMINISTRATION KIT

**Kaspersky® Administration Kit** provides a centralized solution for managing corporate network anti-virus security systems which are based on Kaspersky Lab's applications, such as those comprising Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite. Kaspersky Administration Kit supports all network configurations that use the 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 Kaspersky Lab applications across a network, to computers running Windows. This feature enables the administrator to copy the required set of Kaspersky Lab's applications to a selected computer, and then deploy these applications to the network computers.
- Manage licenses. The administrator can deploy license keys to all installed Kaspersky Lab applications, and from one centralized location, monitor the observance of the license agreement (that is, that the number of applications operating in the network is less than or equal to the number of licenses) and the expiration date.
- Remotely manage Kaspersky Lab's applications on computers running Windows, across a network. The administrator can create a multi-level anti-virus protection system, and manage the operation of all applications from his workstation. This is particularly important for larger companies where the local network consists of a large number of computers that may be located in several separate buildings or offices. This feature enables the administrator to:
  - group computers into *administration groups* based on the functions performed by the computers and on the set of applications installed on them;
  - configure the application settings in a centralized way by creating and applying *group policies*;
  - configure application settings for particular individual computers using the *application settings*.
  - manage the operation of 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 applications, rather than each computer accessing Kaspersky Lab's internet updates server for each individual update. The administrator can schedule automatic updating for all applications, and monitor the installation of updates on client computers.
- Receive reports using a dedicated system. This feature allows the centralized collection of statistics about the operation of all installed Kaspersky Lab applications, and the creation of reports based on the statistics. The administrator can create a cumulative network report about the operation of an application, or reports about the operation of all applications installed on individual computers.
- Use events notification system. The administrator can create a list of events which arise in the operation of applications about which he or she wants to be notified. The list of such events may include, for example, the detection of a new virus, an error that occurred while updating the anti-virus database on a computer, or the detection of a new computer on the network.
- Cooperate with Cisco Network Admission Control (NAC). This functionality provides a mapping between host antivirus protection conditions and Cisco NAC statuses.

The Kaspersky Administration Kit consists of three major components:

- **Administration Server** centralizes the storage of information about Kaspersky Lab applications installed in the corporate network and about the management of these applications. This component supports all Windows applications included in Kaspersky Lab Business Optimal and Kaspersky Corporate Suites. Separate versions of the Network 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 an extension of the Microsoft Management Console (MMC).

## 1.1. The purpose of this document

This Reference Book describes Kaspersky Administration Kit, and contains a step-by-step discussion of its functions. Basic concepts and the general

operation scheme of the application are discussed in the Kaspersky Administration Kit Administrator's Guide.

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 the installation, configuration and functioning of Kaspersky Lab's applications, about removing the most common viruses, and about disinfecting infected files.

## 1.2. Conventions used in this book

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.

| Format feature  | Meaning/Usage  |
|---|--|
| <b>Bold font</b>                                      | Titles of menus, menu items, windows, dialog boxes and their elements, etc.            |
| Note  | Additional information, notes  |
| Attention!  | Information requiring special attention  |
| <i>To perform...</i> ,<br>1. <i>Step 1.</i><br>2. ... | Description of the user's successive steps and possible actions                        |
| <u>Question:</u>                                      | Statement of a problem, example of the demonstration of the application's capabilities |
| [key] – modifier name                                 | Command line modifier  |
| Information messages and command line text            | Text of configuration files, information messages and command line                     |

---

# CHAPTER 2. MANAGING THE LOGICAL NETWORK

This chapter introduces issues related to management of the logical network using Network Agent.

## 2.1. Starting the Administration Console and connecting to the Administration Server

The first issue in using Administration Kit across the network is to locate and connect to the Administration Server.

### 2.1.1. Starting the Administration Console

*To start the application:*

select the **Kaspersky Administration Kit** item in the **Kaspersky Administration Kit** group, on the standard **Start\Programs** menu. This programs group is created only on the administrator's workstations, when Administration Console is installed.

### 2.1.2. Connecting to the Administration Server

*To connect to the Administration Server:*

select the node corresponding to the required server in the console tree.

After this, the Administration Console tries to connect to the Administration Server. If there are several Administration Servers on your network, the Console will connect to the server it last connected to during the previous Kaspersky Administration Kit session. When the application is first launched, it is assumed that Administration Server and Administration Console are running on the same computer. Therefore, Administration Console will try to detect Administration Server on this computer.

If the server is not found, you will be asked to specify the server address manually in the **Connection settings** dialog box (see Figure 1). Enter the required server address in the **Server address** field. You can enter either the IP-address or computer's name in the Windows network.

To connect to the Administration Server through a port that differs from the default one, enter **<Server name>:<Port number>** in the **Server address** field.

Click the **Options** button to show/hide the following advanced connection settings:

- **Use SSL connection.** Select this checkbox to transmit data between the Administration Server and Administration Console via the Secure Sockets Layer protocol (SSL). Unselect this box if you do not want to communicate via SSL. However, this will lower the security of data transmissions against modification or interceptions.
- **Use data compression.** Check this box to increase the rate of data transfer between the Administration Console and the Server, by decreasing the amount of information being transferred and hence lowering the load on the Administration Server.

Enabling this setting will increase the load on the central processor of the computer which is hosting the Administration Console.

- **Use proxy server.** Select this checkbox if you want to connect to the Administration Server via a proxy server. Enter the address for connecting to the proxy server in the **Proxy address** field. Fill in the **User name** and **Password** fields if user authorization is required to access this proxy server.

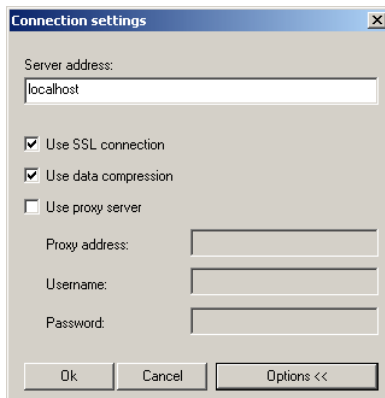


Figure 1. Connecting to the Administration Server

When the connection settings have been confirmed, the Administration Console verifies the user's rights to connect to the Administration Server. If the secure connection is SSL-enabled, the Administration Console authenticates the Administration Server before verifying user rights.

When you connect to the server for the first time, and also if the server certificate for this session differs from your local copy, a request to connect to the server and receive a new certificate will be displayed (see Figure 2). Select one of the following:

- **I want to connect to the server and download the certificate from it** – select this option to connect to the Administration Server and receive a new certificate.
- **I want to specify the certificate file location** – select this option to specify the location of the certificate file, using the **Browse** button. The file has the **.cer** extension and is located in the **Cert** folder in the Kaspersky Administration Kit directory on the Administration Server. The Console will attempt to authenticate the server using the certificate you specified.

You can copy the certificate file to a shared folder or a floppy disk. A copy of this file can be used to configure access settings.

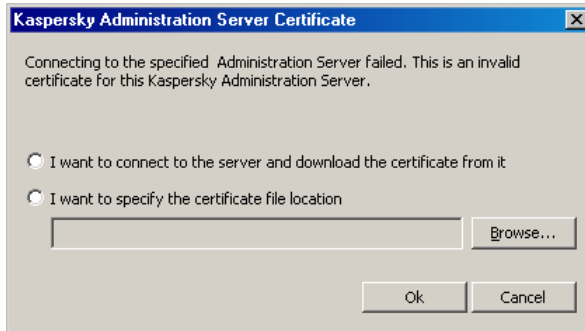


Figure 2. Request to connect to the Administration Server.

User rights are verified using the Windows user authentication procedure. If the user is not authorized to access the Administration Server, i.e. he/she has is not a member of the logical network operators' group (**KLOperators**), or of the administrators' group (**KLAdmins**), try logging on under another account (see Figure 3). In the corresponding form, specify a user account (name and password) which does have logical network operator or administrator rights.

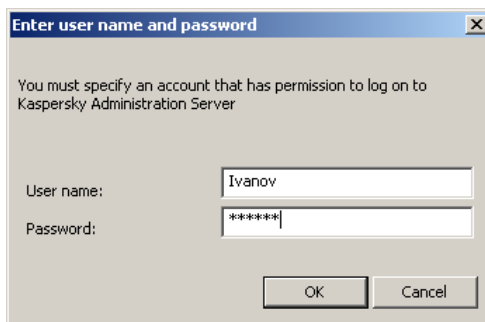


Figure 3. Registering a user to access the Administration Server

If the connection is successful, the logical network structure and settings appear in the console tree.

## 2.1.3. Disconnecting from the Administration Server

*To disconnect from the Administration Server:*

select the **Kaspersky Administration Server (<Server name>)** node in the console tree, and either select the **Disconnect from the Administration Server** command, or use the analogous shortcut menu item in the **Action** menu.

## 2.1.4. Switching between servers

*To connect to another Administration Server:*

select the **Kaspersky Administration Server (<Server Name>)** node in the console tree of the Kaspersky Administration Kit main window, and click the **Logon server** option either on the shortcut menu or on the **Action** menu. In the **Connection settings** dialog box (see Figure 1), enter the name of the server in the logical network on which you plan to work (see above) and, if necessary, check the **Use SSL connection** checkbox to enable secure connection.

If you have no logical network operator or administrator rights for the selected network, access to the Administration Server will be denied.

If the connection to the server is successful, the contents of the corresponding node will be updated.

## 2.1.5. Adding a server to the console tree

*To add a new Administration Server to the console tree*

Select the **Kaspersky Administration Server** node in the Kaspersky Administration Kit main window, and either open the shortcut menu, and click the **New/KAV Server** command, or select this command from the **Action** menu.

As a result, a new node named **Kaspersky Administration Server (<Not connected>)** will appear in the console tree. Use this node to connect to another server installed on your Windows network.

## 2.1.6. Removing a server from the console tree

*To remove an Administration Server from the console tree.*

in the console tree, select the node corresponding to the Administration Server you wish to delete. Either open the shortcut menu and select the Delete command, or select the corresponding item in the **Action** menu.

## 2.2. Granting rights

### 2.2.1. Granting rights to use the Administration Servers

*To grant rights to users to work with the logical network of Administration Server:*

1. Select the node that corresponds to the Administration Server you need in the main Kaspersky Administration Kit window. Either open the shortcut menu and select the **Properties** command, or use the corresponding item in the **Action** menu.
2. Select the **Security** tab in the **Properties: <Server name>** window that opens (see Figure 4).

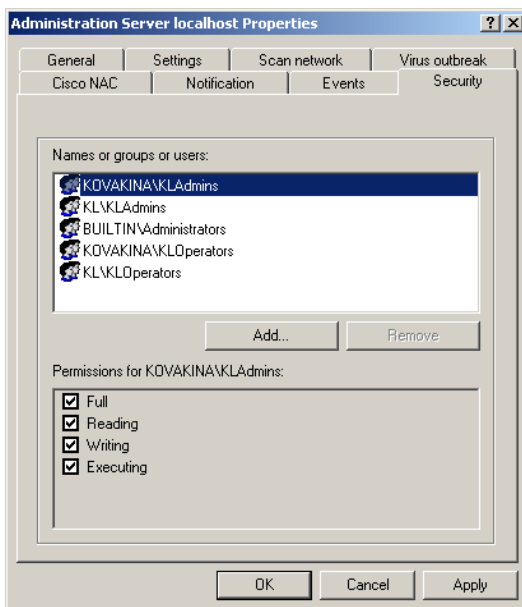


Figure 4. Granting rights to access the Administration Server

The upper part of the tab contains the list of users registered on the computer hosting the Administration Console. The lower part contains the list of possible permissions:

- **All:** includes Reading, Execution and Writing rights.
- **Reading:**
  - connecting to the Administration Server
  - viewing the logical network structure (or administration group);
  - viewing the values of applications' policies, tasks, and settings.
- **Execution:** starting and stopping existing group and global tasks, and report generation.
- **Writing:**
  - creating a logical network, and adding groups and client computers to this logical network (or to an administration group);

- installation of the Network Agent component on client computers;
- creating installation packages for Kaspersky Lab's anti-virus applications, and installing them, and the relevant licenses keys, on client computers;
- updating the version of applications installed on client computers;
- creating policies, tasks for groups and for individual computers, and configuring application settings;
- centralized management of applications, receiving reports about their operation using services provided by the Administration Server, the Network Agent and the Administration Console components;
- granting to users, and groups of users, access rights to the functionality of Kaspersky Administration Kit.

To assign rights, select the required group of users and check boxes next to the names of the permissions being granted. If you wish to check all boxes, check the **All** box.

You can add a new group or a new user by clicking the **Add** button. You can add only users, or groups of users, which are registered within the domain.

3. To confirm the changes to the settings, press the **Apply** or the **OK** button.

## 2.2.2. Granting rights to groups

*To grant rights to work with an administration group:*

1. Select the administration group in the console tree, and either open the shortcut menu and select the **Properties** command, or use the analogous item from the **Action** menu.
2. Select the **Security** tab in the **Properties: <Server name>** window which opens (see Figure 5 ). This tab is similar to the **Security** tab of the Administration Server settings configuration window.

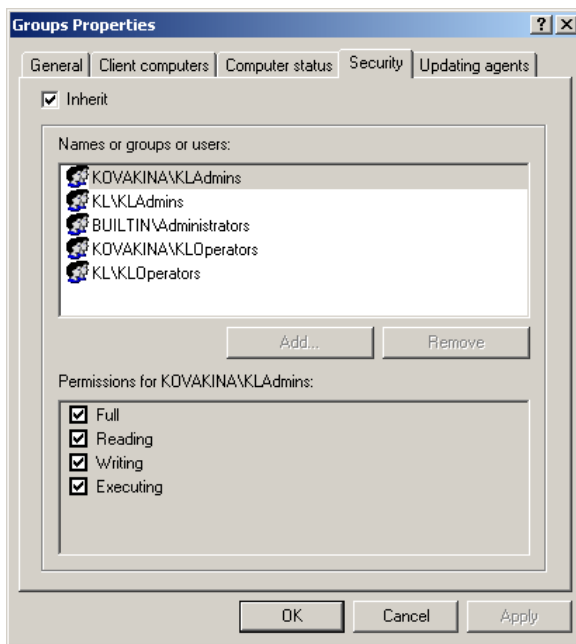


Figure 5. Granting access right to an administration group

Rights for working with the logical network, and all objects included within the network, are configured in the Administration Server network.

To configure individual access rights for an administration group which are different from those specified in the Administration Server settings, uncheck the **Inherit** box.

3. Configure the access rights you wish to grant to the users and groups of users in the list. Rights are granted in the same way as for the Administration Server.
4. To confirm the new settings, press the **Apply** or the **OK** button.

## 2.3. Viewing information about networks and IP subnetworks

### 2.3.1. Viewing information about the computer network

*To view information about the computer network which is, received by the Administration Server during a regular poll:*

Select the **Network** node in the console tree.

Information about the structure of the network, and computers included in this network, is received by the Administration Server through regularly polling of the Windows network and IP subnetworks within the corporate computer network. The content of the **Network** folder will be updated based on the results of this polling.

Initially, after the installation of Kaspersky Administration Kit, the **Network** folder will contain the hierarchy of folders reflecting the structure of domains and workgroups of the corporate Windows network. Each of the folders at the lowest level contains a list of computers, of the respective domain or workgroup, which are not included in the structure of the logical network. The list of computers will be displayed in the results pane. Once a computer is included in any group, information about it will be immediately deleted from the folder. If the computer is excluded from the logical network structure, information about it will again be placed in the corresponding folder of the **Network** node.

Administration Console information updates automatically for nodes only.

To update the data in the result pane, use the **F5** key, the **Refresh** menu, the popup menu options or the **Refresh** link in the task pane.

### 2.3.2. Method for displaying the computer network

*To specify how the computer network will be presented when viewing the **Network** folder:*

select the Network node in the console tree, and select an option from the **View** group in the shortcut menu:

- **Domains** – to display the structure of the computer network as a hierarchy of folders that reflects the structure of domains and workgroups of the Windows corporate network. Each of the lowest level folders contains a list of computers of the respective domain or workgroup which are not included in the structure of the logical network.
- **Active Directory** - to display the network hierarchy that corresponds to the Active Directory structure.
- **IP subnetworks** – to display the computer network as IP subnetworks.

### 2.3.3. Creating an IP subnetwork

*To create a new IP subnetwork*

1. Select the **Network** node in the console tree, and either open the shortcut menu and select the **New/IP subnetwork** command, or use the corresponding item from the **Action** menu.

The **New/IP subnetwork** command is available only when displaying the **Network** folder as IP subnetworks.

2. In the **New IP subnetwork** window that will open (see Figure 6) specify values for the following settings:
  - the name of the subnetwork;
  - how the subnetwork will be described, and values appropriate for the method selected. Select one of these options:
    - **Specify the IP subnetwork using address and the subnetwork mask**; in this case you must specify the **Subnetwork mask** and **Subnetwork address** in the corresponding entry fields.
    - **Specify IP subnetwork using the start and the end IP address**; after this, enter the start and the end IP addresses.
  - a time interval after which information about an inactive computer will be deleted from the Administration Server database, in the **IP address lifetime (hours)** field.

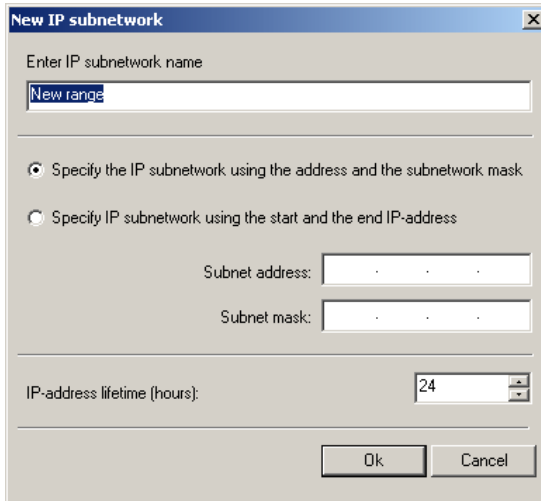


Figure 6. Creating a new IP subnetwork

3. To confirm the settings, press the **OK** button.

## 2.3.4. Viewing and modifying the IP subnetwork settings

*To modify the IP subnetwork settings:*

select the node that corresponds to the required subnetwork in the **Network** folder, and either open the shortcut menu and select the **Properties** command, or use the corresponding item in the **Action** menu.

This will open the dialog window **Properties: <Subnetwork name>** that includes the **General** and **IP ranges** tabs.

You can do the following in the **General** tab (see Figure 7):

- change the subnetwork's name;
- determine whether Administration Server will automatically move new computers, when they are added to the subnetwork, to include them in the structure of the logical network. To do this, check the **Include computer into the structure of the group** box, and specify the administration group using the **Select...** button.

- change the value of the time interval after which information about an inactive computer will be deleted from the Administration Server database, in the **IP address lifetime (hours)** field.
- permit or cancel regular polling of the computers in this subnetwork by the Administration Server. If you do not want the Administration Server to poll the subnetwork, uncheck the **Allow IP subnetwork scanning** box.

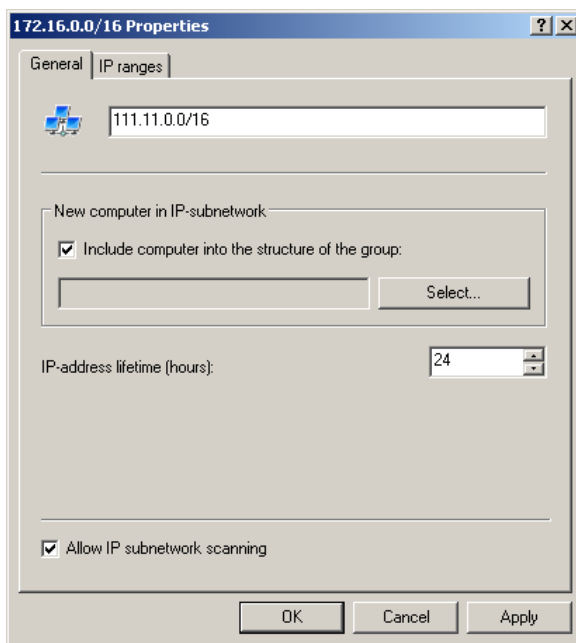


Figure 7. Viewing IP subnetwork settings  
The **General** tab

You can add, edit and delete the IP ranges and masks that define the subnetwork in the **IP ranges** tab (see Figure 8).

- start and end IP addresses of the range;
- subnetwork mask and address.

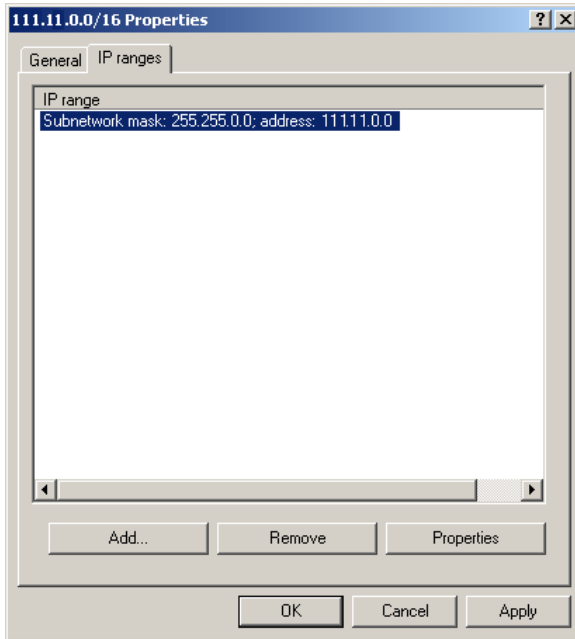


Figure 8. Viewing IP subnetwork settings  
The **IP ranges** tab

To add an IP range that defines the subnetwork, press the **Add...** button. In the **IP ranges** window that opens (see Figure 9) specify the method to define the range, and enter the values for the method selected. Select one of these options:

- **Specify the IP subnetwork using the address and the subnetwork mask**; in this case you must specify the **Subnetwork mask** and **Subnetwork address** in the corresponding entry fields.
- **Specify IP subnetwork using the start and the end IP address**; after this, enter the start and the end IP addresses.

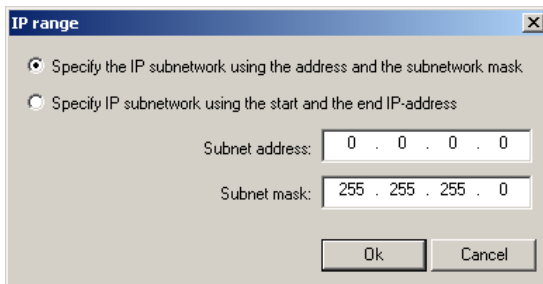


Figure 9. Adding an **IP range**

## 2.3.5. Viewing and Modifying Active Directory Group Parameters

*To modify Active Directory group parameters:*

Under the **Network** folder, select the node representing the desired Active Directory group, and either select **Properties** on the popup menu, or click the corresponding option on the **Action** menu.

This opens the **Properties: <Active Directory Group Name>** dialog containing a **General** tab (cf. Figure. 10). This tab can be used to specify whether the Administration Server will automatically move new computers to the logical network, when they are added to the group. This is accomplished by checking **Include computer into the structure of the group** and specifying the administration group with the **Select** button.

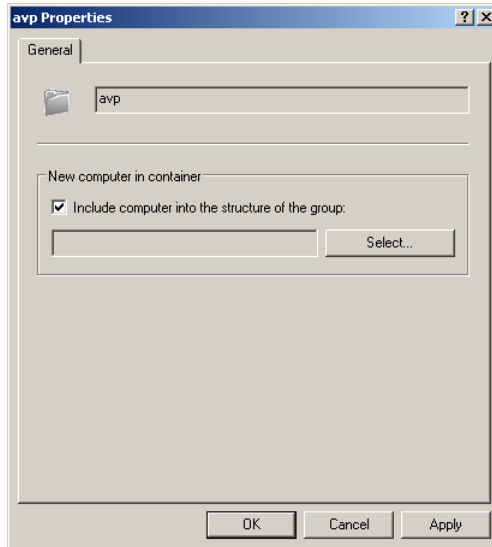


Figure 10. Viewing Active Directory Group Parameters.  
**General Tab**

## 2.4. Quick Start Wizard

### 2.4.1. Using the Quick Start Wizard

*To create a system for the centralized management of antivirus protection:*

1. In the console tree of the Kaspersky Administration Kit main window, select the **Kaspersky Administration Server (<Server Name>)** node. Either click **Quick Start Wizard** on the shortcut menu or on the **Action** menu.
2. Initially the computer network is polled, and computers within this network are identified (see Figure 11). Based on the results of this polling, a service group Network and the structure of the Network folder are formed. The information obtained will be used to automatically create the logical network. To view the structure of the computer network, use the **View network scanning results** hyperlink.

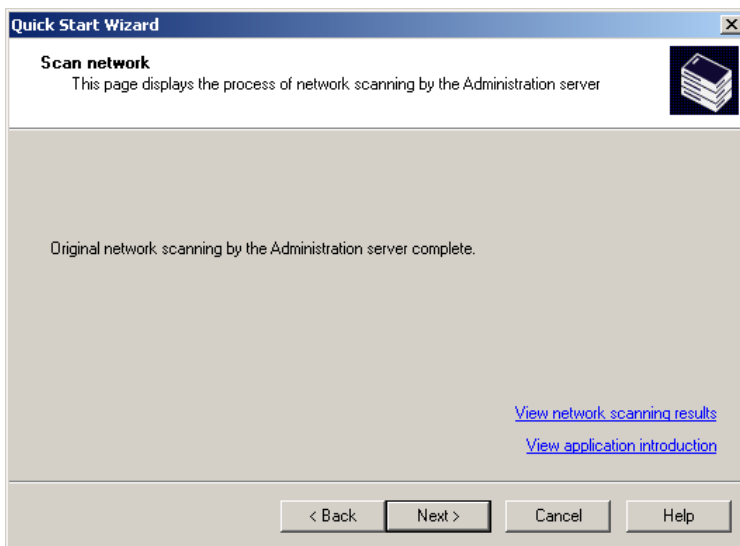


Figure 11. Polling the computer network

3. At this stage you must specify how the logical network will be created (see Figure 12), by selecting one of these options:
  - **Build logical network based on Windows network** – create the logical network automatically, based on the structure of Windows domains and user groups displayed in the **Unassigned** group folder.

If a computer is not available in the **Unassigned** mode when logical network is created (i.e. it is switched off or disconnected from the network), the wizard will not add this computer to the logical network. The computer can be added later when manually configuring the logical network (see section 2.7.1 on page 51).

Creating a logical network using the Quick Start Wizard does not disturb network integrity: new groups are added, but do not replace the existing groups. A client computer that has been already assigned to an existing group will not be added again because the **Unassigned** group displays only computers that are not included in the logical network.

- **Create logical network manually** – create the logical network later.
- **Import logical network from previous version of Kaspersky Administration Kit** – use the logical network structure as it existed in the previous versions of Kaspersky Administration Kit. The restored structure will be as follows: servers and groups will be imported as administration groups, and workstations attached to each server will be added as members of the corresponding administration group.

To import the structure of the previous logical network, the application uses data stored on the main server in the configuration file **ncd.dat**. This file is located in the folder **NCD**, in the **Kaspersky Administration Server** installation folder. If the Administration Server is currently installed on the same computer which previously hosted the main server, this configuration file will be found automatically. If the Administration Server is unable to find the **ncd.dat** file, select it manually using the **Browse...** button.

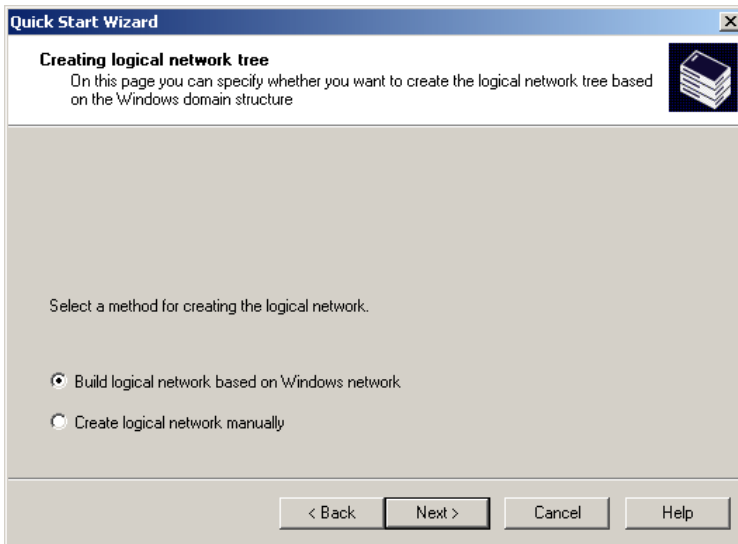
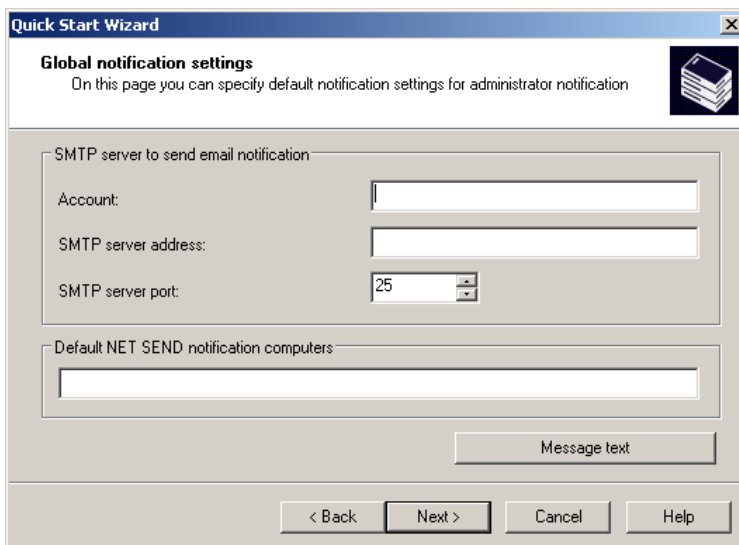


Figure 12. Specifying how the logical network will be created

4. In the next wizard box (Figure 13), configure settings for sending alerts, generated by Kaspersky Lab applications, via e-mail and NET SEND. Also, use the **Message text...** button to create a template for alert messages (for more details, see section 3.1.1.2 on page 66).

These settings will be used as the default settings for application policies.



The image shows a Windows-style dialog box titled "Quick Start Wizard" with a close button in the top right corner. The main heading is "Global notification settings" with a sub-heading "On this page you can specify default notification settings for administrator notification" and a small icon of a stack of papers. The dialog is divided into two main sections. The first section, titled "SMTP server to send email notification", contains three input fields: "Account:" (a text box), "SMTP server address:" (a text box), and "SMTP server port:" (a spinner box with "25" selected). The second section, titled "Default NET SEND notification computers", contains a large empty text box. Below this section is a button labeled "Message text". At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 13. Configuring how notifications are forwarded

5. In the next stage, you should configure the anti-virus protection system (Figure 14).

The Quick Start Wizard creates a anti-virus protection system for logical network clients, using versions 5.0 and 6.0 of Kaspersky Anti-Virus for Windows Workstations. In this case, the Administration Server creates a policy and defines a minimum set of tasks for the highest hierarchical level of versions 5.0 and 6.0 of Kaspersky Anti-Virus Virus for Windows Workstations, and global tasks to retrieve updates for the Administration Server and to copy backup data.

The following objects will be displayed:

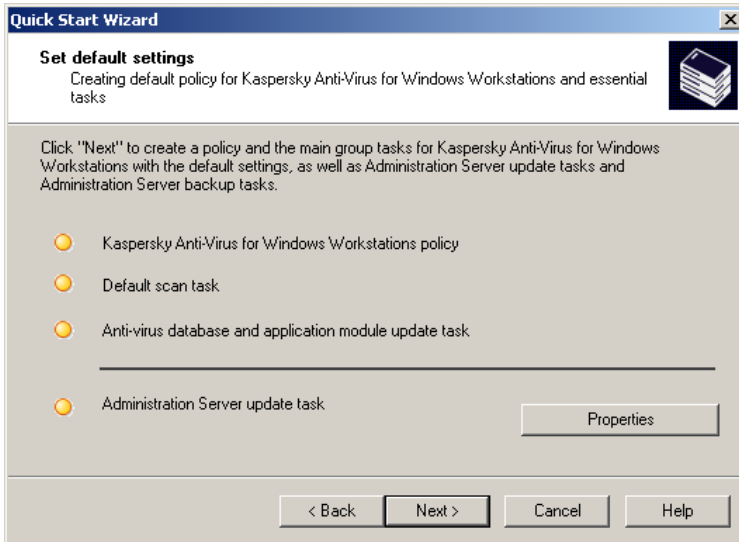


Figure 14: Configuring the anti-virus protection system

- policies for versions 5.0 and 6.0 of Kaspersky Anti-Virus for Windows Workstations in the Policies folder of the Groups group. The policies will be named **Policy for Kaspersky Anti-Virus 5.0 for Windows Workstations** and **Policy for Kaspersky Anti-Virus 6.0 for Windows Workstations** and will have default settings.
- In the **Global Tasks** node of the console tree, there is a global task for updating the Administration Server. This policy is called **Download updates task** and has default settings.
- The task of copying backup data of the **Administration Server** is in the **Global Tasks** node of the console tree, with the name **Backup copying of Administration Server** and with default settings.
- The tasks for updating the anti-virus database for versions 5.0 and 6.0 Kaspersky Anti-Virus for Windows Workstations is in the **Tasks** folder of the **Groups** task, with the names **Anti-Virus database and application modules update task** and **Update task (version. 6.0)**, and have default settings.
- The on-demand scan tasks for versions 5.0 and 6.0 of Kaspersky Anti-Virus for Windows Workstations are in the **Group tasks** folder of the **Groups** group with the names **On-demand**

**scan task** and **Virus detection task (version 6.0)**, and have default settings.

Policies for versions 5.0 and 6.0 of Kaspersky Anti-Virus 5.0 for Windows Workstations are not created if policies for these applications already exist in the **Groups** folder.

If group tasks for the **Groups** group and the global updating task with these names already exist, these tasks will not be formed at this time.

If necessary, you can customize updating options. To do so, click on the **Updater settings...** button, and specify the required values in the dialog box that appears on your screen (for more details see section 4.1.2 on page 147).

Click **Next**. The wizard window displays the process of creating the tasks and the policies. If errors occur, an error message will be displayed.

6. Select in the next window of the wizard (see Figure 15):
  - **Yes, I want to start Download Updates Task now.** The task for retrieving updates by the Administration Server will be run after the Quick Start Wizard has completed.
  - **No, I don't want to start Download Updates Task now.** The updating task will be run according to the schedule specified in the settings of the global task called **Retrieving updates by the Administration Server**.
7. In the final window of the wizard you can launch the **Deploy wizard**. You can use this wizard to install the Network Agent. If you do not wish to install the application immediately after the Quick Start Wizard is completed, uncheck the **Launch the Deploy Wizard** box.

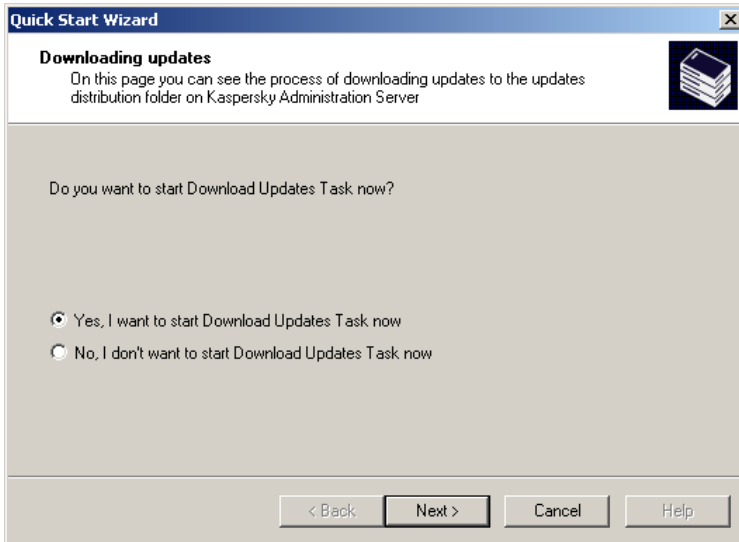


Figure 15. Quick start wizard.  
Configuring retrieving of the update

## 2.5. Creating, viewing and configuring a logical network

### 2.5.1. Viewing information about groups

*To view information about the structure of a group that is a part of the logical network group:*

Select the desired group folder in the **Groups** folder: a list of objects included in this group will be displayed in the details panel. You can also expand the corresponding branch of the console tree.

- To view information about group policies, select the **Policies** folder. If policies are applied to the selected group, they will be displayed in the details panel; otherwise the details panel is empty.
- To view information about group tasks, select the **Tasks** folder. If tasks are defined for the selected group, they will be displayed in the details panel; otherwise the details panel is empty.

- To work with the logical network of the slave Administration Server, select the **Administration Servers** folder.
- A list of clients included in the selected group is displayed in the details panel.

To refresh the client list in the result pane, use either the **F5** key, the **Refresh** option on the menu or a popup menu, or the **Refresh** link in the task pane.

## 2.5.2. Viewing group properties, and configuring interactions between client computers and Administration Servers

*To view the group's properties, and the settings defining the interaction between the Administration Server with the client computers that are a part of the group:*

select a folder with the name of the required group in the **Groups** folder, and then use either the **Properties** command from the shortcut menu, or from the **Action** menu. This will open the **<Group name> Properties** dialog box, which has the tabs: **General**, **Computers**, **Computer status**, **Security** and **Update Agents**.

The **General** tab (Figure 16) displays the following information:

- Group name.
- Parent group name that includes the current group. For the **Groups** group this field contains the name of the Administration Server of the logical network which contains it.
- Statistical information about the group structure – the number of nested groups and the total number of clients, including clients in nested groups.
- Creation date.
- Date when the name or attributes of the group were last modified. If the group name and group properties have not changed since it was created, the value is **<Unknown>**.

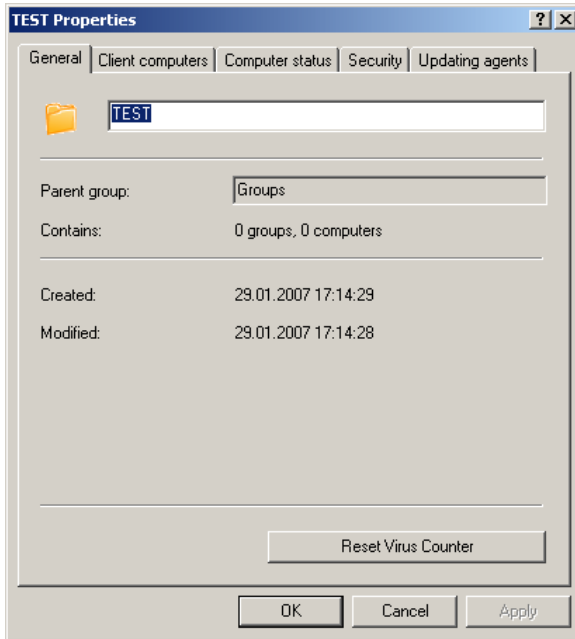


Figure 16. The **General** tab

Click the **Reset virus counter** button to reset the virus detection counter for all client computers in the group.

The **Computers** tab (Figure 17) displays the following information:

- The **New client computer in the group** section shows which applications can be automatically installed on client computers that are added to the group. If the box next to the application's name is checked, it will be automatically installed.

For the **Unassigned** group properties and its subgroups (see Figure 29), the **New client computer in the group** section contains the checkbox **Add computer to group**. If this checkbox is checked, new computers on the Windows network will be automatically included to the logical network group specified in the text field below.

- The **Client computer activity in the network** section specifies how Administration Server reacts to the inactivity of client computers. After the specified time periods have elapsed, the logical network administrator can be notified and the computers can be deleted from the group.

- The **Move computers from domain Active Directory group or IP subnet** option determines whether the Administration Server will automatically add all new client computers to the administration group, when they are detected during network polling.

To enable this option, check the box and using the **Select** button specify the Active Directory group or IP subnetwork from which new computers will be moved.

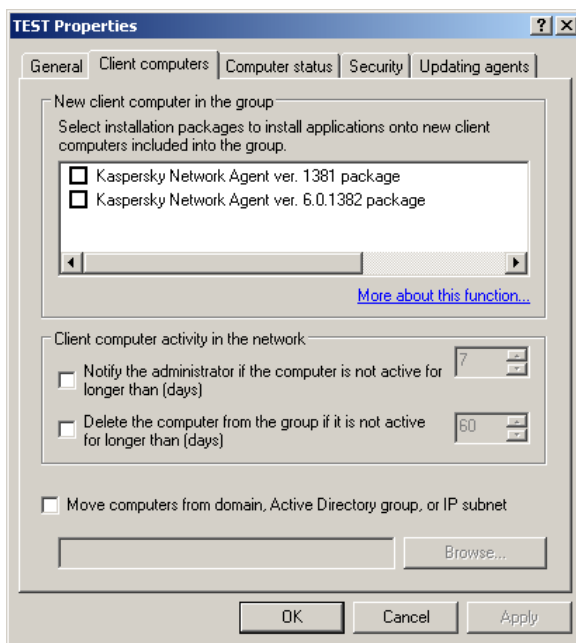


Figure 17. Viewing group properties. The **Computers** tab

The **Computer status** tab specifies criteria for determining whether a client computer requires attention, based on the status of the computer's anti-virus protection and on the level of its network activity. If at least one of these conditions has not been met, the client computer will be assigned one of the statuses: **Critical** or **Warning**. If the client computer does not meet any of the above conditions, it will be assigned **OK** status.

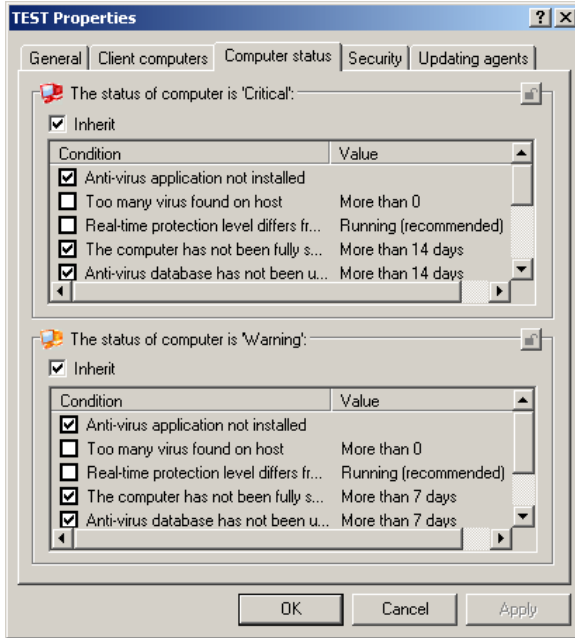





Figure 18: The **Computer status** tab

You can change the threshold values for some of the conditions, by selecting the required condition in the Condition column and double-clicking it to open the editing window (see Figure 19).

For example, you can establish the maximum number of days during which the client computer has not connected to the Administration Server. After this period of time is elapsed, the computer is assigned **Critical** status.

If the computer status is **OK**, a green icon  will appear next to its name, for example in the main application window. If the computer has the **Warning** status, a yellow icon  will be displayed. If the computer status is **Critical**, a red icon  will be displayed.

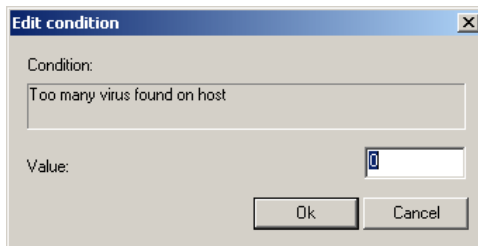


Figure 19. Modify computer status

The criteria for determining the status of the client computer are set in the setting of the parent group level, and will be inherited by all groups of the logical network. To configure individual criteria for a group, uncheck the **Inherit** box and configure the settings.

On the **Security** tab (see Figure 5), specify the rights of users, and groups of users, when working with the administration group (see section 2.2.2 on page 18).

On the **Updating Agents** tab (see Figure 110) a list of computers used to distribute updates and installation packages within the group will be created (see section 4.2.3 on page 151).

### 2.5.3. Viewing information about the client computer

*To view information about a logical network client:*

Select the group in the **Groups** folder that contains the desired client. The list of clients in this group will be displayed in the details panel (you can also expand the corresponding branch in the console tree). Select the required client and either click **Properties** on the shortcut menu or on the **Action** menu. This will open the **<Computer name > Properties** dialog box, which has several tabs (Figure 20).

To find the client computer you need, you can use the **Find** function (see section 5.6 on page 180).

On the **General** tab (Figure 20), you can do the following:

- View the network settings of client computers.
- Obtain information about the computer in the System Information window (cf. Figure 20) which is accessible through the **Sys-**

**tem** link. The **Totals** tab of this window contains general information about computer settings and the operating systems installed, and the **Applications** tab lists the external applications installed on the computer.

- Edit the host name. The host name is generally assigned by the Administration Server; it coincides with the computer name on the Microsoft Windows network.
- Enter your own description for the computer;
- Define connection settings with the Administration Server by using the **Do not disconnect from the Administration Server** checkbox. If the checkbox is checked, the client-server connection is permanent. By default, the client-server connection is established periodically for synchronizing or transmitting data.

Note that permanent connection should only be provided for the most important clients, because the total number of simultaneous connections supported by the Administration Server is limited to several hundreds.

The information displayed on the tab reflects data received during the last synchronization session.

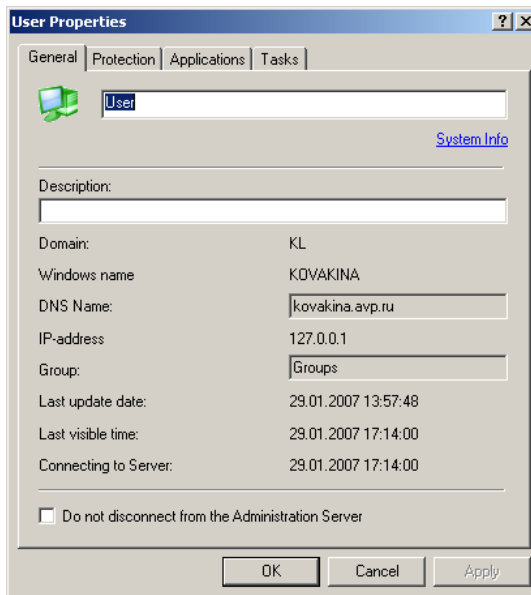


Figure 20. Viewing client properties. The **General** tab

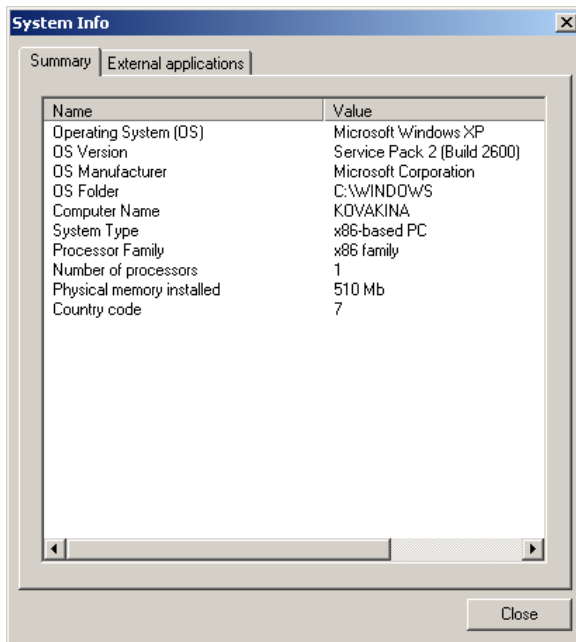


Figure 21. Viewing system characteristics of a client computer

The **Protection** tab (Figure 22) shows the current status of anti-virus protection on a client computer. You can view the following data:

- **Real-time protection status** – current status of anti-virus protection.
- **Last full scan date** – date and time of the last virus scan.
- **Viruses found** – total number of viruses detected, from the first scan until the virus counter was reset. To reset the counter, click **Reset virus counter** on the shortcut menu or on the **Action** menu.
- **Computer status** – the status of the client computer according to the diagnostics criteria of the computer's anti-virus protection, and the criteria regarding the level of computer network activity, set by the administrator. The **Computer status description** field lists the conditions which determined the client computer's current status.

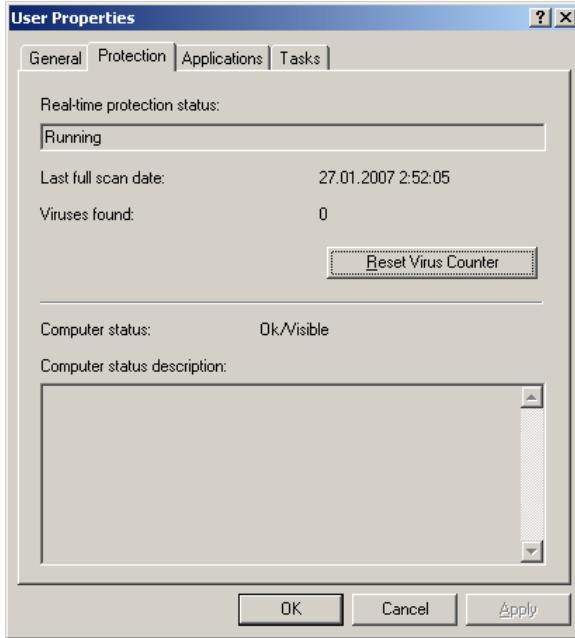


Figure 22. Viewing system characteristics of a client.  
The **Protection** tab

The **Applications** tab lists all Kaspersky Lab applications installed on the client computer. You can view general information about an application, manage its performance, and configure its settings (for details, see section 3.1.1.2 on page 66).

On the **Tasks** tab, you can manage tasks for client computers (view existing tasks, delete and create new tasks, start and stop them, change task settings, and view task performance results). The information about tasks reflects the data received during the last client-server synchronization session. The Administration Server queries the client for current task status. If connection fails, the status is not displayed.

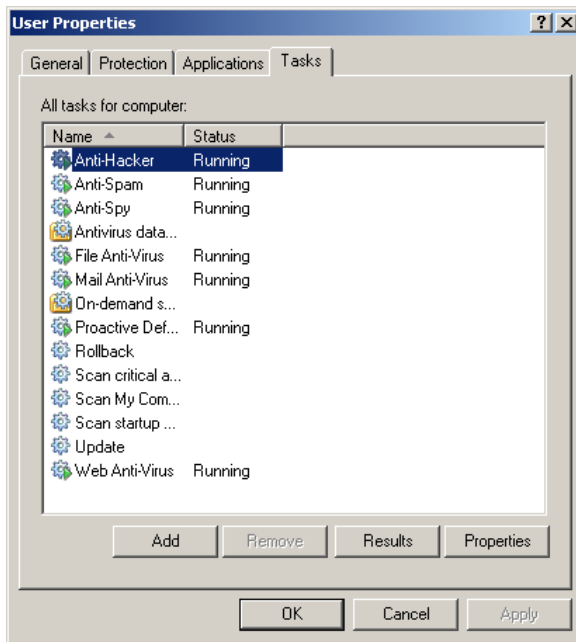


Figure 23. Viewing system characteristics of a client. The **Tasks** tab







## 2.5.4. Viewing the logical network of a slave Administration Server

*To view the logical network of a slave Administration Server via the logical network of the main server, connection the Console to the slave server:*

1. In the console tree of the main Administration Server, select the **Administration servers** node in the folder of the required group.
2. In the **Administration servers** node, select the required slave Server, and either select the **Connect to the Administration server** command from the shortcut menu, or use the corresponding command from the **Action** menu.

The Administration console will reflect the structure of the logical network of the slave Administration Server, allowing you to view the structure of the logical network using the regular method (see section 2.5 on page 32).

The slave Administration Server inherits from the main Server all the group tasks and policies of the group to which it belongs. Inherited policies and tasks are indicated on the slave Server as follows:

- the icon  will be displayed next to the names of policies inherited from the main Administration server. The regular policy icon is .
- the settings of the inherited policy will not be accessible for changes on the slave Server.
- settings that are specified as not modifiable in the inherited policy are indicated by the “locked” icon  in all application policies on the slave Server, and use values specified in the inherited policy.
- values of the settings that are not “locked” in the inherited policy are indicated by the “unlocked” icon . If the setting is specified as modifiable in the slave Server policy, it can be changed in the application settings (see section 3.1.1.2 on page 66) or task settings (see section 3.2.4 on page 124).
- the icon  will be displayed next to the names of group tasks received from the main Administration Server. The regular task icon is .

Policies and tasks received by the slave server from the main Administration Server are not available for modification.

Global and group deployment tasks cannot be transferred to slave Administration Servers.

*To view the logical network of the slave server directly using the Console:*

add computer on which the slave Administration Server is installed to the console tree as a new server (see section 2.8.1 on page 59) and connect to it (see section 2.8.1 on page 59).

## 2.6. Groups

### 2.6.1. Adding a group

*To create a group:*

1. In the **Groups** folder of the console tree, or in the results pane, select the group folder in which the new group will be included. If

- you create a group at the highest hierarchy level, select the **Groups** folder.
2. Open the shortcut menu and use the **New / Group** command, or select the corresponding command in the **Action** menu.
  3. Enter the group name in the window that will open (Figure 119) and press the **OK** button.

The new folder with the specified name should appear in the **Groups** node in the console tree. This new folder will automatically contain nested folders for **Policies, Group tasks** and **Administration servers**, which will be filled later by defining group policies, creating group tasks and adding slave servers.

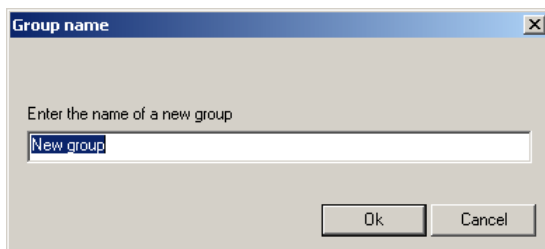


Figure 24. Creating a group

## 2.6.2. Configuring group settings

*To configure group settings:*

1. Select the required group in the console tree or in the results pane, and use the **Properties** command in the shortcut menu or the corresponding item in the **Action** menu.
2. This will open the group configuration window (see Figure 25) which contains the following tabs: **General, Client computers, Computer status, Security** and **Updating Agents**.

You can change the group name using the **General** tab (see Figure 25). This name must be unique at this level of hierarchy among the groups. Additionally, the following information is provided:

- **Parent group:** the name of the group that includes this group. For the highest hierarchy group this field contains the name of the Administration Server for the logical network to which this group is related.
- **Contains:** statistical information about the structure of the group, including the number of nested groups and the total

number of the client computers including those in nested groups.

- **Created:** the group creation date.
- **Modified:** the date of the last change of the group's name or attributes. The field contains value **<Unknown>** if the name and attributes of the group have not been changed.

Click the **Reset Virus Counter** button to reset the counter for the viruses detected on all client computers in the group.

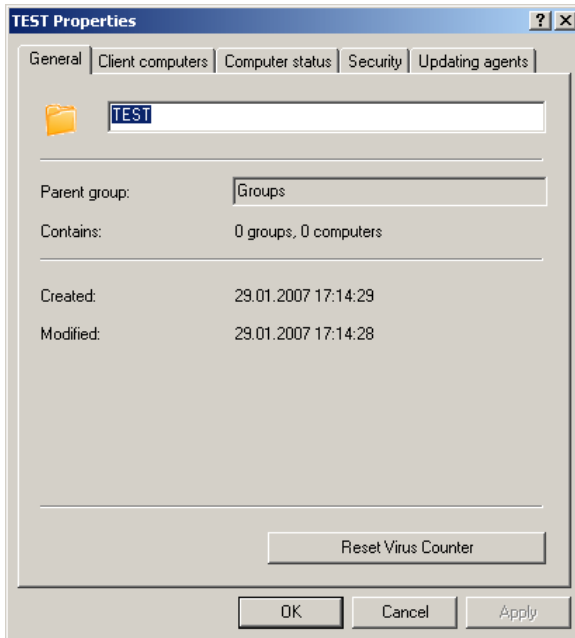


Figure 25. Configuring group settings.  
The **General** tab

The following settings can be configured on the **Client Computers** tab (see Figure 26):

- In the **New client computer in the group** section shows which Kaspersky Lab applications can be automatically installed on client computers that are added to the group. If the box next to the application's name is checked, it will be automatically installed.

To automatically install Kaspersky Lab applications on new computers running the operating systems Microsoft Windows 98/ME, Network Agent must have been installed on these computers.

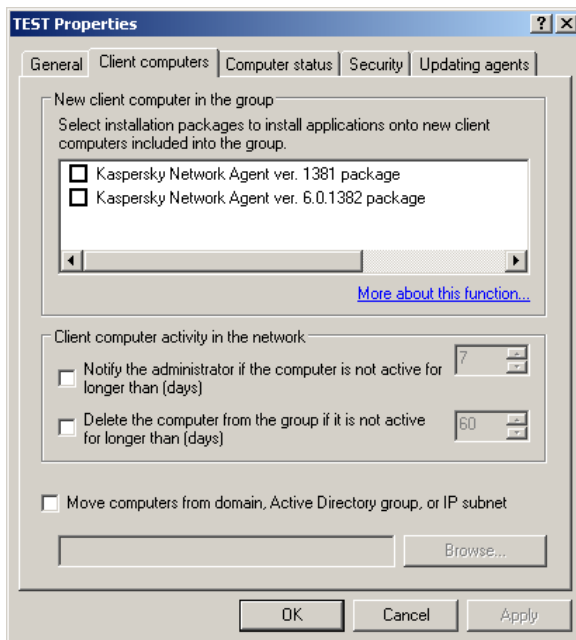


Figure 26. Configuring group settings.  
The **Client computers** tab

- The **Client computer activity in the network** section specifies how the Administration Server reacts to the inactivity of client computers of this group.
  - if you wish the logical network administrator to be notified after a period of inactivity, check the **Notify the administrator if the computer is not active for longer than (days)** box and specify the number of days in the field to the right of the box.

Notification shall be performed in accordance with the settings specified in the properties of the Administration Server, on the **Notification** tab (see Figure 67).

- if you wish inactive client computers to be deleted from the group, check the **Delete the computer from the group if it is not active for longer than (days)** box and specify the number of days in the field to the right of the box. Once the specified period has elapsed, the client computer will be automatically deleted from the group and moved to the **Network** group.
- The **Move computers from domain, Active Directory group or IP subnet** box determines whether the Administration Server will automatically add all new client computers detected during the network polling to the administration group.

Using the **Select** button, specify the Active Directory group or the IP subnetwork from which new computers will be moved.

The **Computer status** tab (see Figure 27) specifies criteria for determining whether a client computer will be assigned one of the statuses: **Critical** or **Warning**. If the client computer does not match any of the conditions listed, it will be assigned the status **OK**.

For some conditions the threshold values may be changed, by selecting the required condition in the **Condition** column and double clicking it to open the editing window.

For example, you can specify the maximum number of days during which the client computer has not connected to the Administration Server. After this length of time has elapsed, the computer is assigned **Critical** status.

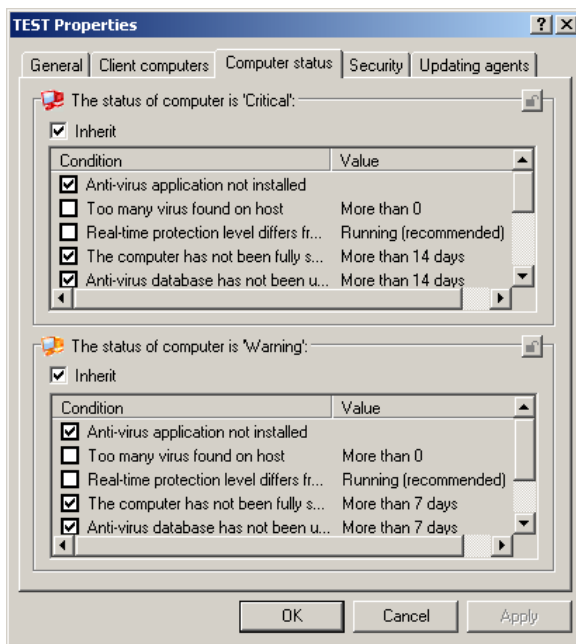





Figure 27. Configuring group settings.  
The **Computer status** tab

If the computer status is **OK**, then an  icon will be displayed next to its name, for example in the main application window. If the computer has the **Warning** status, a yellow icon  will be displayed. If the computer status is **Critical** status, a red icon  will be displayed.

The criteria for determining the status of the client computer are set in the settings at the level of the parent group, and are inherited by all groups in the logical network. To establish individual criteria for a group, uncheck the **Inherit** box and configure the settings. For groups at the top of the hierarchy, the **Inherit** box is disabled.

On the Security tab (see Figure 27) specify the rights of users, and groups of users, when working with the administration group.

Rights for working with the logical network, and all objects included in the structure of the network, are configured in the Administration Server settings (see section 2.2 on page 16). To configure individual access rights for an administration group that are different

from those specified in the Administration Server settings, uncheck the **Inherit** box.

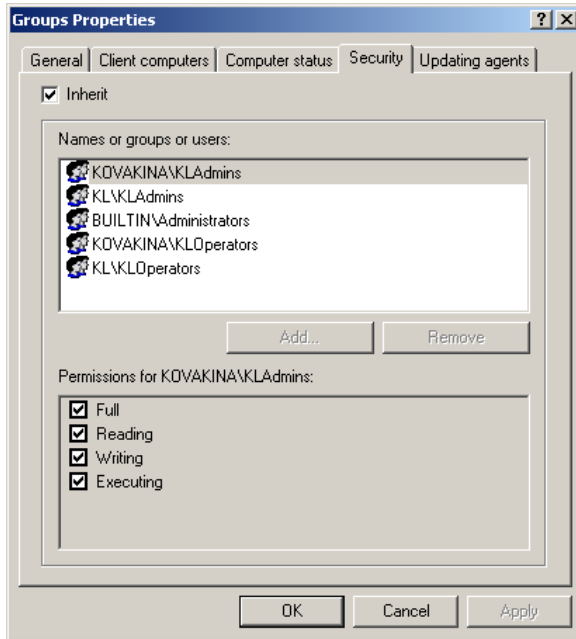


Figure 28. Configuring group settings.  
The **Security** tab

The upper part of the tab contains the list of users registered on the computer hosting the Administration Console. The lower part contains the list of possible permissions:

- **All:** includes Reading, Execution and Writing rights.
- **Reading:**
  - connecting to the Administration Server;
  - viewing the structure of the logical network (or administration group);
  - viewing the values of the applications' policies, tasks, and settings.
- **Execution:** starting and stopping existing group and global tasks, and report generation.

- **Writing:**
  - creating a logical network, and adding groups and client computers to this logical network (or to an administration group);
  - installation of the Network Agent component on client computers;
  - creating installation packages for Kaspersky Lab anti-virus applications, and installing them, and the relevant license keys, on client computers;
  - updating the version of applications installed on client computers;
  - creating policies, tasks for groups and for individual computers, and configuring application settings;
  - centralized management of applications, receiving reports about their operation using services provided by the Administration Server, the Network Agent and the Administration Console components;
  - granting to users, and groups of users, access rights to the functionality of Kaspersky Administration Kit.

To assign rights, select the required group of users and check boxes next to the names of the permissions you wish to grant. If you wish to check all boxes, check the **All** box.

You can add a new group or a new user by clicking the **Add** button. You can add only users, or groups of users, which are registered on the Administration Console computer. To delete a group or a user from the list, use the **Delete** button.

Using the Updating Agents tab (see Figure 109) create, if required, a list computers that will be used to distribute updates and installation packages within the group (see section 4.2.3151). Using updating agents decreases the load on the administration servers.

To confirm the changes to the group settings, press the **Apply** or the **OK** button.

### 2.6.3. Configuring automatic installation of software on new computers in the group

*To ensure automatic installation of Kaspersky Lab applications on new computers in the group:*

1. in the **Groups** folder, select the folder with the name of the required group, and either open the shortcut menu and select the **Install** command, or use the corresponding item in the **Action** menu.
2. A **Properties:<Group name>** window will open. On the **Client computers** tab (see Figure 17), in the group **New client computer in the group** check boxes beside the names of installation packages that will automatically install the software. Uncheck boxes if no installation is required. By default no software is automatically installed. For all installation packages for which boxes are checked, deployment group tasks with names like **Installation <Name of the selected installation package>** will be created. You can run these tasks manually.

For automatic installation of Kaspersky Lab applications on new computers running Microsoft Windows 98/ME, Network Agent must have been installed on these computers.

In the future you can change the name of the group, move it to another group or delete it.

### 2.6.4. Moving groups

*To move a group:*

in the console tree or in the results panel, select the required group folder and use either the standard **Cut / Paste** commands of the shortcut menu, similar items in the **Action** menu, or perform the same operation using the mouse.

### 2.6.5. Renaming groups

*To rename a group,*

in the console tree or in the results panel, select the required group folder and use the **Properties** command in the shortcut menu, or the

corresponding item in the **Action** menu. Rename the group using the General tab of the **Properties:<Group name>** window that will open (see Figure 16).

You cannot rename the **Groups** folder because it is an in-built element of Administration Console.

## 2.6.6. Deleting a group

*To delete a group from the logical network,*

in the console tree or in the results panel, select the required group folder and use the **Delete** commands in the shortcut menu or in the **Action** menu.

A group can only be deleted if it does not contain slave servers, nested groups or client computers.

## 2.7. Client computers

### 2.7.1. Adding computers to the logical network

*To add a computer/computers to the logical network,*

1. In the **Group** folder, select the group folder to which you wish to add the client computer. If you are adding a client computer to the highest hierarchy level, select the **Groups** folder.
2. Either open the shortcut menu and use the **New Computer** command, or use the corresponding command in the **Action** menu. This will launch the corresponding wizard.
3. The first stage is to define which method to use to add the computer:
  - automatically– based on data received by the Administration Server while polling the corporate Windows network. The computer will be moved from the **Network** folder to the corresponding group.
  - manually– based on data entered by the administrator. The reliability and accuracy of the information will be verified to pre-

vent naming conflict. If the Administration Server database contains information about the presence of a computer in the Windows network, the computer will be included in the group.

4. You will then be asked to create a list of computers to be included in the group.

If you selected the automatic method for adding computers, the wizard window will contain the **Network** folder. Select computers to be included in the group. You can select computers from different folders, or select entire folders.

If you selected the manual method for adding computers, you will be asked to create the list of computers to be included in the group. You can either create the list of addresses in the wizard window using the **Add** and **Remove** buttons, or import the list from a text file using the **Import** button. You can use either IP address, a range of IP addresses, or computer names on the Windows network as the computer's address. To import the list from a file, specify a *txt* file with the list of addresses being added by the computer. Each address must be located on a separate line.

Once the wizard completes successfully, the computers will be included in the group and will be displayed in the results pane under names determined by the Administration Server.

A computer can also be automatically added in the main application window of Kaspersky Administration Kit by dragging the computer from the **Network** folder and dropping it in the logical network folder, with the mouse.

## 2.7.2. Automatically adding new computers to a group

*To ensure that all new computers detected within the Windows network are automatically added to a certain administration group by Administration Server,*

open the **Network** group's **Properties** window and select the **Client computers** tab (see Figure 29). In the **New computers in the network** section, check the **Include computer into the structure of the group** box and using the **Browse...** button, select the group to which new computers will be added.

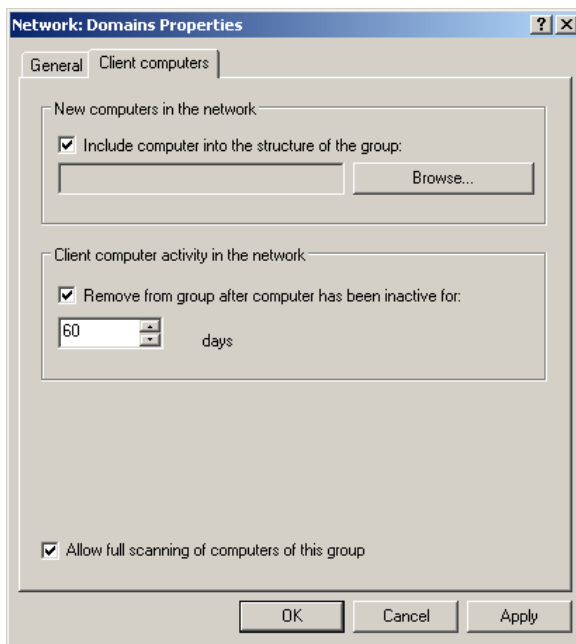


Figure 29. Viewing the **Network** group properties.  
The **Client computers** tab

You can move client computers from one group to another by excluding them from the logical network, using either the standard shortcut commands **Cut / Paste** and **Delete** or analogous items from the **Action** menu. Computers deleted from the logical network will be moved to the **Network** group.

The moving operation can also be performed using the mouse.

### 2.7.3. Moving a client computer to a different logical network. Administration Server change task

*To create an Administration Server change task:*

1. Connect to the Administration Server administering the logical network which contains the computers to be moved (see 2.1 on page 11).

2. Start the group or global task creation wizard (for details, see section 3.2.1 on page 112, and 2.2.2 on page 18).
3. Select **Kaspersky Network Agent** and **Change Kaspersky Administration Server Task**, as the application and the task type respectively (see Figure 30).

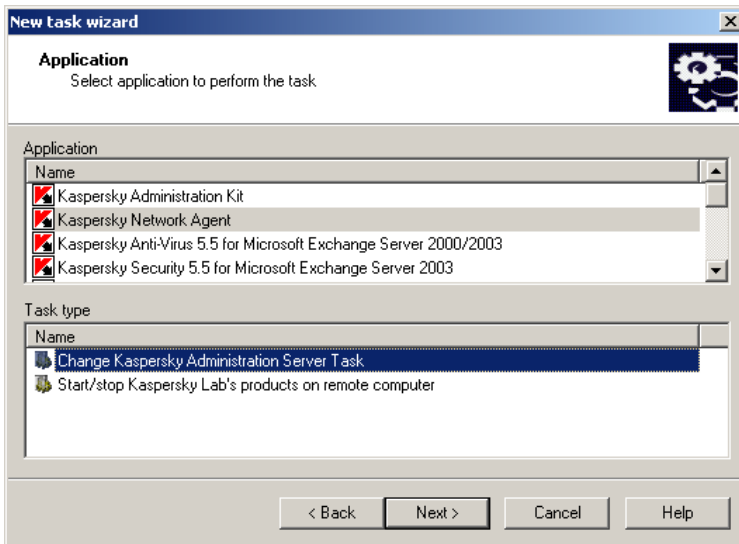


Figure 30: Selecting the application to be installed

4. During the next stage (see Figure 31), specify the settings that will be used by the Network Agent installed on client computers to connect to the new server.

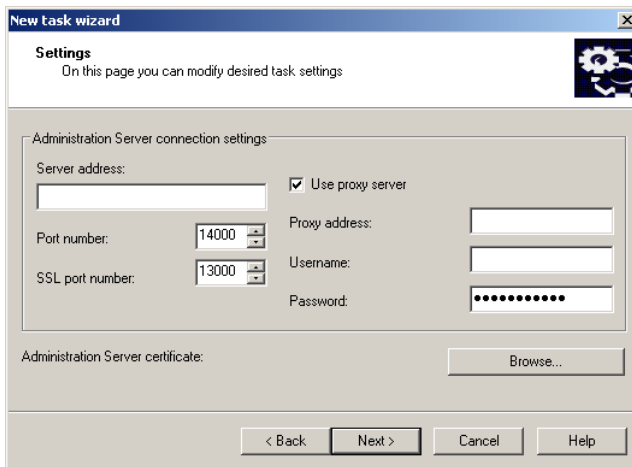


Figure 31: Specifying the server and selecting the certificate

In the **New Kaspersky Administration Server Location** group of fields:

- specify the address of the Administration Server in the logical network to which the client computers are going to be moved, using either the IP address or the computer's name on the Windows network.
- specify the port number to be used for connection to the new Administration Server.
- specify the port number to be used for secure connection to the new Administration Server (using the SSL protocol).
- check the **Use proxy server** box if you are connecting to the Administration Server via a proxy server. Enter the proxy server address in the **Proxy server address** field, and fill the **User name** and **Password** fields if user authentication is required to access the proxy server.

Next, click the **Change certificate...** button, and specify in the resulting **Kaspersky Administration Server certificate** window the certificate file to be used for authentication on the new Administration Server.

The certificate file has the extension **.cer**, and is located in the **Cert** subfolder of the Kaspersky Administration Kit installation folder, on the Administration Server to which the computers are being moved. You can copy the certificate file to a public access file or to a disk, and use this copy to configure the access parameters to the server.

Task settings configured at this stage can be modified on the **Settings** tab (see Figure 31) of the task property window (details of the task settings configuration see section 3.2.4 on page 124.

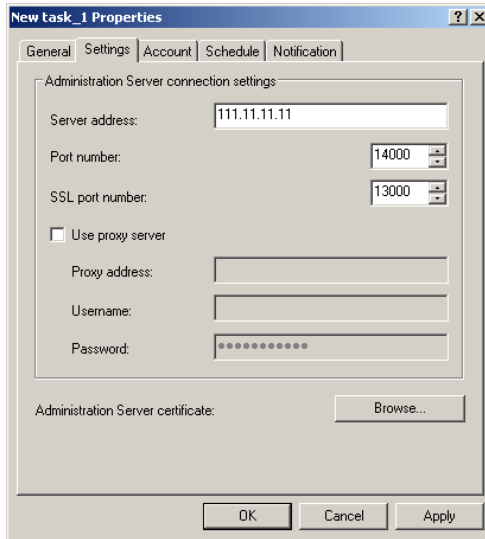


Figure 32: Viewing the Administration Server change task settings:

5. If you are launching a global task, you must create a list of client computers on which this task will be run (see section 3.2.2 on page 122). When the task successfully completes, these computers will be moved to the logical network of the Administration Server specified in the task settings, and put into the **Network** group.

If a group task, is used all client computers of the specified group will be connected to the new Administration Server.

The Administration Server change task will not be created and executed for the client computer which hosts Administration Server.

6. Specify the profile under which the task will be run (see section 3.2.1 on page 112).
7. During the final step create the schedule for running this task (see Section 3.2.1 on page 111 for details).

## 2.7.4. Manually connecting the client computer to the Administration Server. The *klmover.exe* utility

To manually connect a client computer to the Administration Server:

using the command line on the client computer, start the **klmover.exe** utility included in the Network Agent installation.

After the installation of Network Agent, this utility is located in the component's root installation folder, and when run from the command line can perform the following actions, depending on the command line parameters used:

- connects the Network Agent to the Administration Server using the parameters supplied;
- logs the results of the operation in the events log file, or displays them on the screen.

Utility command line syntax:

- **klmover [-logfile <filename>]<sup>1</sup> [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-noss!] [-cert <path to the certificate file>] [-silent] [-dupfix]**

The command line parameters are as follows:

- **-logfile <filename>** – record the results of the program's operation in the log file. By default the information will be stored in the file stdout.tx. If the modifier is not used, the results and error messages will be printed to the screen.

---

<sup>1</sup> {Entries in square bracket are optional modifiers.}

- **-address <server address>** – the address of the Administration Server for connection. The address can be represented by IP address, NetBIOS or DNS name of the computer.
- **-pn <port number>** – number of the port that will be used for an unsecured connection to the Administration Server. The default value is 14000.
- **-ps <SSL port number>** – number of the port that will be used for a secured connection to the Administration Server using the Secure Sockets Layer (SSL) protocol. The default value is **13000**.
- **-noss1** – use an unsecured connection to the Administration Server; if no modifier is used, a secure connection to the Network Agent will be established using the SSL protocol.
- **-cert <full path to the certificate file>** – use the specified certificate file for authentication when accessing the new Administration Server. If no modifier is used, the Network Agent will receive the certificate on its first connection to the Administration Server.
- **-silent** – launch the utility in non-interactive mode. This modifier can be useful, for instance, when launching the utility from the launch scenario when registering the user.
- **-dupfix** – this modifier is used if the Network Agent was installed using a method other than the regular method by using a distribution package. For example, it could have been restored from a drive image.

## 2.7.5. Verifying manual connection of the client computer to Administration Server The *klnagchk.exe* utility

To verify connection of the client computer to the Administration Server:

using the command line on the client computer, start the ***klnagchk.exe*** utility included in the Network Agent installation.

After the installation of Network Agent, this utility is located in the component's root installation folder. When run from the command line it can perform the following actions, depending on the command line parameters used:

- output, to the screen or in the log file, the connection parameters used by the Network Agent installed on the client computer to connect to the Administration Server;

- output to the screen or in the log file, statistics about the operation of Network Agent, since its last launch, and the results of this utility's operation;
- attempts to connect the Network Agent to the Administration Server;
- if the connection could not be established, sends an ICMP packet to verify the status of the computer on which the Administration Server is installed.

Utility command line syntax:

- **knagchk [-logfile <filename>]<sup>2</sup> [-sp] [-savecert <path to the file certificate>] [-restart]**

The command line parameters are as follows:

- **-logfile <filename>** – log the connection parameters used by Network Agent to connect to the Administration Server and the results of the utility operation. By default the information will be stored in file **stdout.tx**. If the modifier is not used, the parameters, results and error messages will be printed to the screen.
- **-sp** – display the password used to authenticate the user on the proxy server. This parameter is used if connection to the Administration Server is performed using a proxy server.
- **-savecert <filename>** – save the certificate used to access the Administration Server in the specified file.
- **-restart** – restart the Network Agent after the utility is completed.

## 2.8. Slave Administration Servers

### 2.8.1. Adding a new slave Administration Server

*To add a slave Administration Server to the logical network:*

1. Select the **Administration Servers** node in the administration group, and either select the **New Administration Server** item on the shortcut menu, or click the same option on the **Action** menu. A wizard will start.

---

<sup>2</sup> {Entries in square bracket are optional modifiers}

2. You will need to type the name of the slave server. The new Administration Server will be displayed under this name in the administration group. The name must be unique within this level of the hierarchy.
3. At the next stage of the wizard, specify the network address of the slave Administration Server. After this, the master Administration Server will connect to the slave server and transfer all properties, including the network address and certificate of the master Server, and the slave server's name.

If you do not want to specify the network address of the slave Server, just click **Next**.

4. Specify the certificate of the slave Administration Server. Click **Browse** and locate the certificate file.
5. If you previously specified the slave server's address, this stage will enable you to specify the settings for connecting the slave Administration Server to the main server.
  - Specify the address of the main Administration Server. You can use either its IP address or computer's name in the Windows network as the computer's address.
  - If a proxy server is used for connection, configure the connection settings in the **Proxy server settings** group of fields.

Check the **Use proxy server** box. Enter the proxy server address in the **Proxy server address** field. Fill the fields **User name**, **Password** and **Confirm password** if user authentication is required to access the proxy server.

If the address of the slave server has not been specified, this step will be skipped.

6. The following actions are performed during the next step:
  - information about the slave Server is added to the main Administration Server's database;
  - the Administration Console connects to the slave Server;
  - the settings used to connect the slave Administration Server to the main server are configured.

If the slave server's address has not been specified, you will have to perform the following steps manually after the wizard has completed:

- connect the Administration Console to the slave Server;

- configure the connection between the slave Administration Server and the main server.

Press the **Next** button. The progress of the action will be displayed in the wizard window. If an error occurs an error message will be displayed.

7. Press the **Finish** button in the last window of the wizard.

When the wizard completes the main Administration Server will add information about the slave server to its database. The icon and the name of the slave Server will be reflected in the **Servers** folder. in the corresponding administration group.

## 2.8.2. Configuring the connection of the slave server to the main server

*To configure the connection of a slave server to the main Administration Server,*

1. Add the slave Administration Server to the console tree as a managed Administration Server (see section 2.8.1 on page 59).
2. In the **Properties:Administration server <computer name>** window that will open, click the **Server hierarchy settings** hyperlink on the **General** tab.
3. In the **Master server settings** window that will open, check the box **This administration server is a slave server**.

After this, in the **Master server connection** group of fields:

- Specify the address of the main Administration Server. You can use either IP address or the computer's name in the Windows network as the computer's address.

If you are connecting via a proxy server, check the **Use proxy server** box. Enter the proxy server address in the **Proxy server address** field. Fill the fields **User name**, **Password** and **Confirm password** if user authentication is required to access the proxy server.

To apply the new settings press the **Apply** or the **OK** button.

4. Press the **Apply** or **OK** button in the **General** tab in the **Properties:Administration server <computer name>** window.

As the result the slave Administration Server will connect to the main server and will receive from it all policies and tasks for the group to which

the slave Server now belongs. After this you can connect to the slave Server via the main server from the **Administration Server** node.

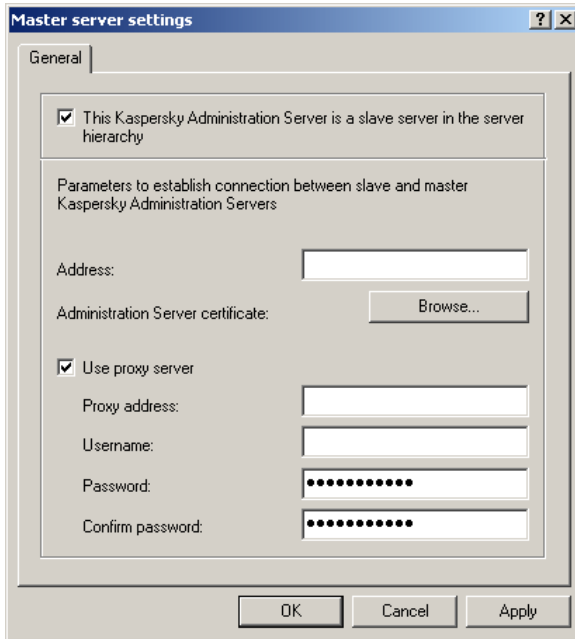


Figure 33. Configuring the slave Administration Server's connection to the main Administration Server.

---

# CHAPTER 3. REMOTE APPLICATION MANAGEMENT

## 3.1. Configuring application settings

### 3.1.1. Managing policies

#### 3.1.1.1. Creating a policy

*To create a new group policy*

1. In the console tree, select a group for which you want to create a policy. In this group folder, select the **Policies** folder and click the **New/Policy** item on the shortcut menu or the **Action** menu to start a new policy wizard. Follow the wizard's instructions.
2. At this stage, you must specify the policy name and the application for which this policy is being created.

Enter the policy name. If a policy with this name already exists, the **\_1** ending will be automatically added to the end of the name of the new policy.

Select an application from the **Choose the application for which to define a policy** drop-down list. The drop-down list includes all applications that have their Console Plug-ins installed on the administrator workstation.

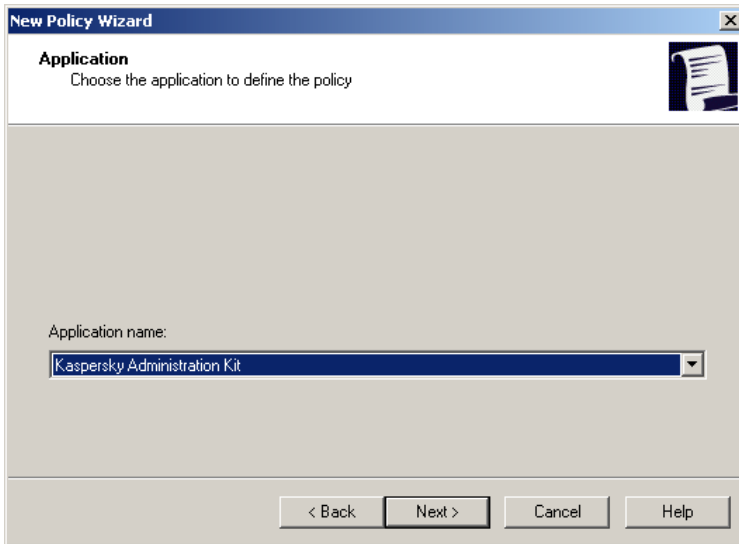


Figure 34. Creating a policy. Selecting an application

3. Specify the policy status in the next wizard window (see Figure 35) from these following options:
  - **Active policy.** The policy being created will be used as the application's current policy.
  - **Inactive policy.** The policy will be saved in the **Policies** node. If required, it can be activated (see section 3.1.1.4 on page 79).
  - **Mobile user policy.** This policy will be applied after you disconnect the computer from the corporate logical network. This type of policy is available for Kaspersky Anti-Virus for Windows Workstations 5.0 and 6.0, Kaspersky Anti-Virus for 5.0 for Windows File Servers and Kaspersky Anti-Virus for 6.0 for Windows Servers.

There can be several policies created in a group for one application, but only one policy can be the active policy.

Activating one policy makes the previously active policy inactive.

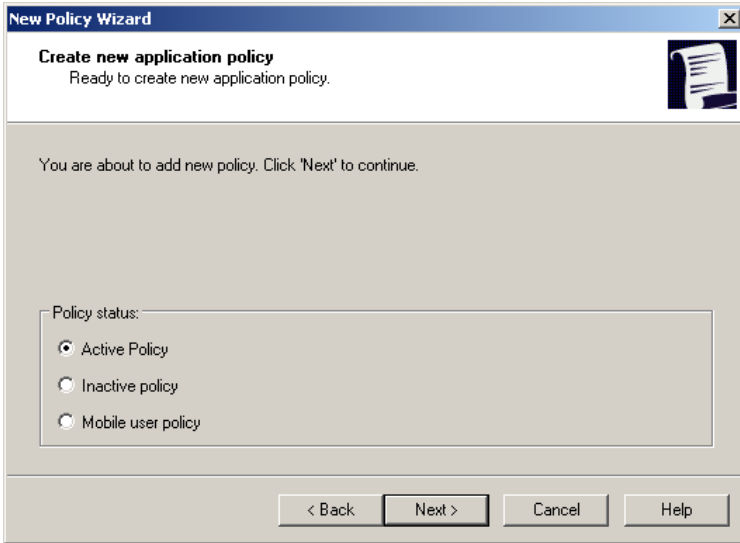




Figure 35. Creating a policy. Activating the policy

4. Next you must specify the general settings for the policy and edit settings for the selected application (Figure 36). You can lock policy settings for nested groups, application settings, or task settings. Policy settings that can be locked are marked with the  icon. To lock a setting, click this icon. The icon will change to .

**Local application settings have a higher priority than policy settings. For a policy to take effect on client computers, you should lock certain parameters.**

When creating a policy, you can only specify a minimum set of parameters required for operation of the application. All other settings are set to the default values applied during the local installation of the application. The policy created can be modified later (see section 3.1.1.2 on page 66).

For more information about configuring the policy for each application, refer to the corresponding documentation.

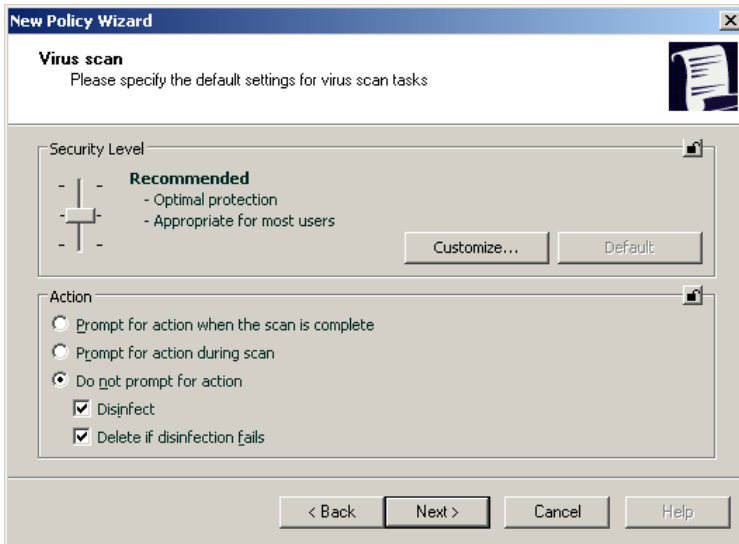


Figure 36. Creating a policy for Kaspersky Anti-Virus 6.0 for Windows Workstations

5. Press the Finish button in the last window of the wizard.

Once a policy is created, parameters which may not be modified (are "locked") are applied on clients to which the policy applies.

Additional configuration can be performed in the **Advanced** window (cf. Figure 39) to edit other policy parameters which apply to client application and task settings.

### 3.1.1.2. Viewing and configuring policy settings

*To view group policy settings and/or modify them:*

In the console tree, choose the required group and select the **Policies** folder in this group. In the details pane, you will see a list of all policies created for this group. Choose the policy required, and click the **Properties** command on the shortcut menu or on the **Action** menu.

You will see the **<Policy name> Properties** dialog box with several tabs in which you can configure a group policy for an application. The contents of the tabs are specific to each application, and their description is provided in the documentation for the applications. Note that the **General**,

**Enforcement**, and **Event processing** tabs are common for all applications.

The **General** tab (Figure 37) displays general information about the policy:

- policy name.
- name of the application for which the policy is created (for example, Kaspersky Anti-Virus 5.0 for Windows Workstations).
- application version.
- creation date and time.
- date and time of last modification.
- the **Activate policy based on the event** box and the list used to select an event that triggers the policy activation.
- the drop-down **Policy status** list, in which you can specify whether the policy is an active policy, inactive policy or a policy for a mobile user.

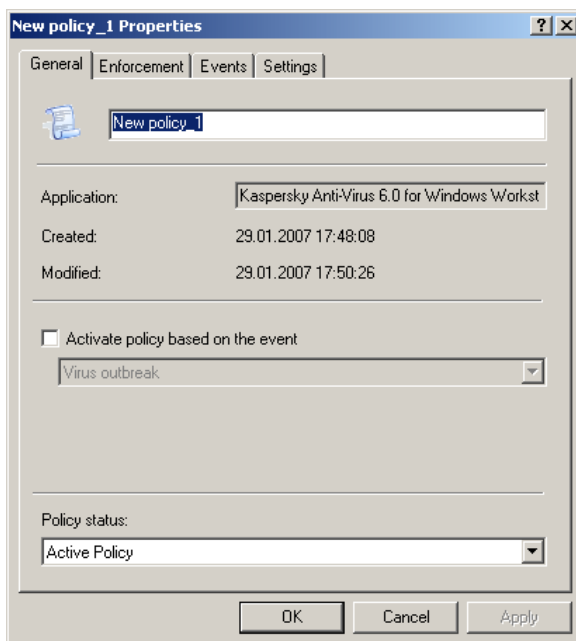


Figure 37. Editing a policy. The **General** tab



On this tab you can:

- change the policy's name;
- determine the automatic activation of the policy upon a certain event and select such event;
- set the policy status.

The **Enforcement** tab (Figure 38) displays the results of enforcing the policy on client computers in the group. The tab shows the numbers of computers for which the policy was:


- defined
- enforced
- pending
- failed

In the section **Changing optional settings**, you can specify which settings, in the application and task settings, will be changed in the policies of nested groups after the policy was first enforced. If the box **Change optional application settings after the policy is first enforced** is:


- not checked, when the policy is first enforced, only mandatory unlocked application settings (indicated by the  icon) will change. To prevent users modifying mandatory settings on client computers, left-click the icon. The icon will change to .
- checked, all application settings will be changed according to the policy settings. Just as with the previous option, you can prevent the user changing mandatory settings.


The local settings will be changed automatically once the policy is first enforced on the client computer. If you would like to reapply the policy with modified settings, press the **Change now** button.

The lower section of the **Policy Application** tab (see Figure 38) may be used to configure replication of policy parameters into client application and task settings. Follow the **Advanced** link and select one of the options below in the resulting window (cf. figure 39):

- **Leave Unchanged.** This would cause only parameters marked with  under policy settings to be applied to an application. Remaining parameters will be governed by local settings. This is the default option.

If a policy is deleted or revoked, applications will revert to values in effect before the policy was applied.

- **Modify Non-Optional Parameters when Policy is First Applied.** This would result only in parameters marked in the policy with a  being enforced with respect to an application.

If a policy is deleted or revoked, only parameters editable under the policy (i. e. those marked with ) will revert to their original values.

- **Modify all Parameters when Policy is First Applied.** This would cause all local parameters to assume values as per policy settings.

After a policy is deleted or revoked, the application will continue with policy-defined settings. Settings may subsequently be modified manually.

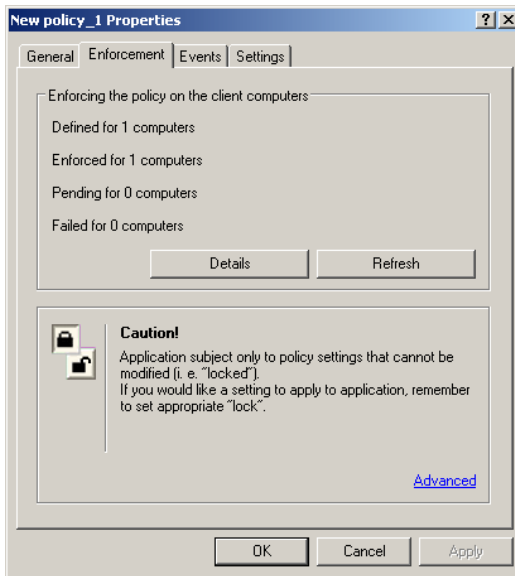


Figure 38. Editing a policy. The **Enforcement** tab

Local parameters are modified automatically based on the option selected when a policy is first applied to a client.

If some policy values have been modified and need to be reapplied, click **Modify Now**. This will cause the policy to be applied based on the parameter selected above.

Applying a policy to a large number of clients will significantly increase the load on the Administration Server and the amount of network traffic.

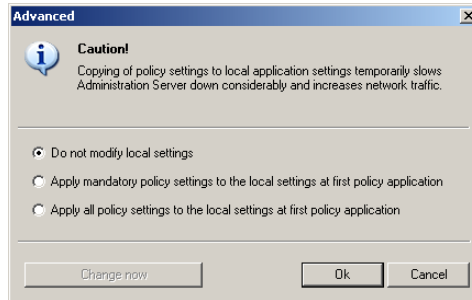


Figure 39. Policy Application Configuration

Detailed information about the results of policy enforcement on each client is available in the dialog box (Figure 40), accessed by clicking the **Details** button. The **Details** dialog box displays a table that has the following columns:

- **Computer** – client name
- **Domain** – name of the domain to which the client belongs
- **Status** – the policy status, which may have one of the following values:
  - **Pending** – settings for this policy have been changed on Administration Server, but they were not yet synchronized with this computer;
  - **Finished** – the policy for an application on this computer has been successfully applied;
  - **Scheduled** – the policy for an application on this computer has not been applied yet;
  - **Failed** – the policy for an application on this computer has failed (the computer was turned off, disconnected, the application did not run, or was not installed).
- **Date** – date and time when the event occurred.

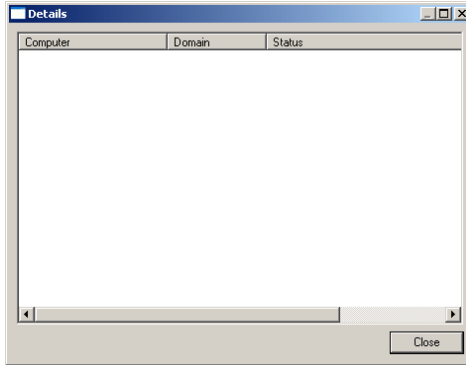


Figure 40. Information about policy enforcement on clients of one group

The **Events** tab (Figure 41) defines rules for handling application-related events – what type of events to record, how to notify the administrator or other users upon virus protection-related events, and where to store event logs.

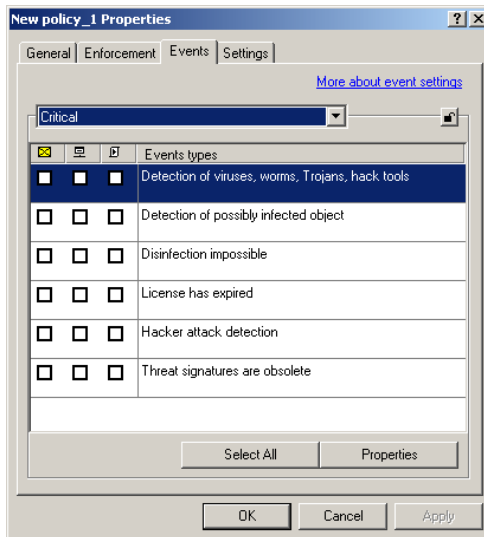


Figure 41. Editing a policy. The **Events** tab




After the policy has been created, the values on the **Events** tab will match the default application settings. The settings are specific to each

Kaspersky Lab application, and more information about them is available in user guides for each application. If necessary, you can change the policy settings as needed.

For all Kaspersky Lab applications, events related to anti-virus protection may have the following severity levels:

- **Critical** – a critical event: for example, detection of a virus.
- **Functional failure** - for example, an internal error
- **Warning** – a warning message: for example, detection of a suspicious object or a password protected archive.
- **Informational message** - for example, the level of real-time protection has changed.

Rules for handling events are defined for each level of severity:

1. From the drop-down list, select the severity level: **Critical**, **Error**, **Warning**, or **Info**.
2. Events corresponding to the selected severity level will be displayed in the table below. The list of events is specific to each application. For more information about events, see the application documentation. Select the types of events to be recorded by pressing the **Shift** and **Ctrl** keys on your keyboard. Click **Select All** to select all event types.
3. To enable notification of selected events, specify the notification methods by checking appropriate columns in the table ( – electronic mail,  – NET SEND facility,  – run an executable). Then click the **Properties** button for the selected event type and go to the **Notification** tab (see. Figure 42).

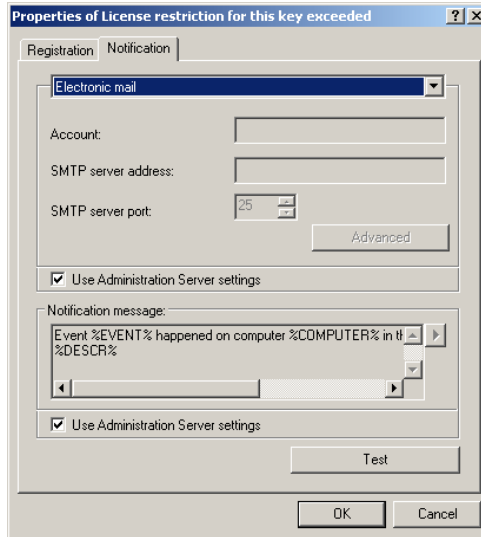


Figure 42. Editing event properties. **Notification** Tab.

The upper section of the tab is used to configure notification methods. If the **Use Administration Server Settings** checkbox is checked, the values specified on the **Notifications** tab under Administration Server properties are used by default. To modify notification settings, uncheck **Use Administration Server Settings** and select from the drop-down window:

- **Electronic Mail** (see Figure 68). Under this option:
  - Enter the notification recipient's email address in the **Recipient Address** field. Several addresses can be entered as a list separated by commas or semi-colons;
  - Enter the email server address in the **SMTP Server Address** field. An IP address or a Windows network name may be used;
  - Enter the SMTP server connection port number under **SMTP Server Port Number**. Port 25 is used by default;
  - Enter the sender and subject line for the message that will be delivered as notification. Click the **Advanced** button and complete the **From** and **Subject** fields in the resulting dialog (see Figure 43). Use the same window to enter **User Name** and **Password** in the relevant fields if ESMTP authorization is being used.

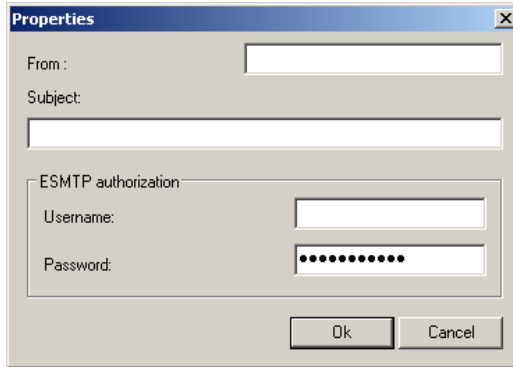


Figure 43. Configuring Notification Settings.  
Specifying Sender and Subject line

- **NET SEND** (cf. Figure 44). Under this option, use the field below to enter recipient host addresses for network notifications. An IP address or a Windows network name may be used. Several addresses may be entered as a list, separated by commas or semicolons.

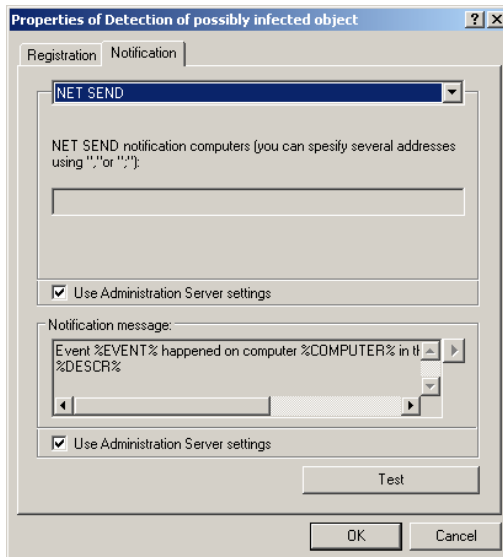


Figure 44. Configuring notification.  
Notification using NET SEND

- **Run Executable** (see. Figure 44). Under this option, use the **Browse** button to select an executable to run when an event is triggered.

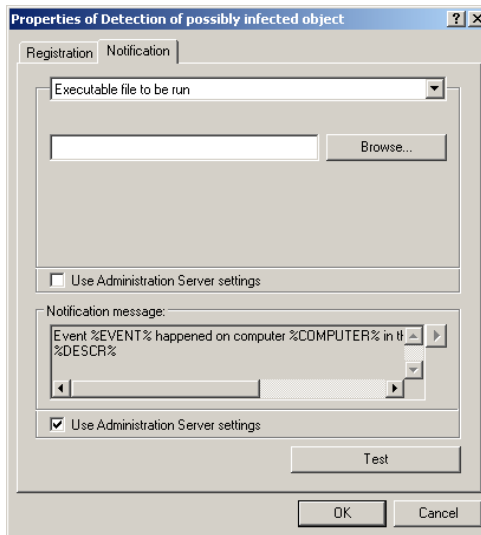



Figure 45. Configuring notification.  
Notification using executables

Executable environment variable names are the same as the names of the placeholders used to create the message text (see. Figure 44).

At the bottom of the tab enter the message which will be delivered as notification. If the **Use Administration Server Settings** checkbox is checked, the message text specified on the Administration Server's **Notification** tab will be used by default. To modify the message, uncheck **Use Administration Server Settings** and enter a new message.

Information about a logged event may be included in the message. Enter appropriate placeholders by selecting them from a drop-down list accessible, through the  button:

- **Event Severity Level.**
- **Source Computer.**

- o **Domain.**
- o **Event.**
- o **Description.**
- o **Logged at.**
- o **Task Name.**
- o **Application.**
- o **Version Number.**
- o **IP address.**
- o **Connection IP address.**

A test message may be sent to test the values entered on this tab , by clicking the **Test** button. This will cause a test notification send window to open (cf. Figure 46). In the event of errors, detailed error information will be displayed.



Figure 46. Configuring notification parameters  
Sending a test notification

4. To record event information in event logs, select the event types and click the **Events** button. Select the **Logging** tab (cf. Figure 47) and select the options below:

- check the **Store events on the server for (days)** checkbox to make the Administration Server log events that occur on all clients in the group. In the field on the right, specify the number of days that the server will store information. When the specified period has elapsed, the entry corresponding to this event will be deleted. You can view event logs stored on the Administration Server through the Administration Console on the administrator workstation. The events are logged in the **Events** node of the console tree.
- check the **Store events locally** checkbox to save events locally on each client. In this case, you can only view event logs through the locally installed Administration Console (Local computer node).
- **In Client Windows Event Log**, to save event information in the each client computer's Windows system log.
- The **Store events in server's Windows Event Log** checkbox to enable logging all virus protection-related events on all clients in this group in the specified Administration Server's Windows Event Log.

This option is available only for Kaspersky Anti-Virus 5.0 for Windows File Servers.

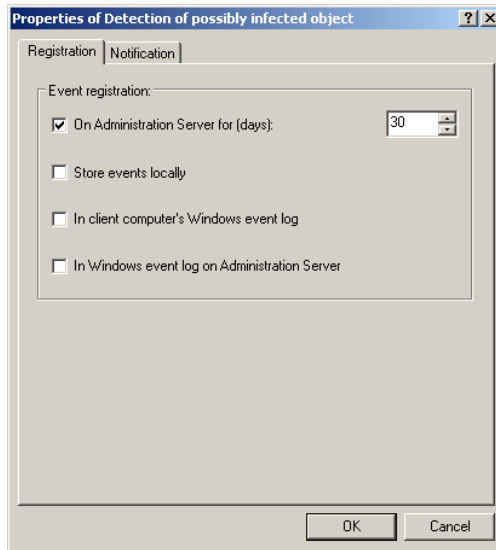


Figure 47. Configuring event logging methods


The information in Windows event logs can be viewed using **Event Viewer**, a standard Windows event management tool.

5. After all required settings have been configured, click Apply and proceed to the next severity level.

### 3.1.1.3. Displaying Inherited Policy in Nested Group Result Panel

*To have inherited policies display in a nested group under the **Policies** folder:*

1. Select the **Policies** folder in a nested group's result pane.
2. Open popup menu, select the **Type** option, and check **Inherited Policies**.

This will cause inherited policies to be displayed in the result pane marked with . Inherited policy properties may be viewed. Editing of inherited policies is only available within the group under which they were created.

### 3.1.1.4. Activating a policy

*To apply a group policy as the active policy for the application,*

1. Select the required group policy in the results panel and either select the **Properties** command from the context menu, or use the corresponding item in the **Action** menu.
2. In the group policy settings **Properties: <Policy name>** box which opens, switch to the **General** tab (see Figure 37).
3. Select the **Active policy** item in the drop down list of the **Policy status** field.

To deactivate the policy, select the **Inactive policy** item..

4. Press the **Apply** or **OK** button.

### 3.1.1.5. Activating a policy based on an event

*To activate a group policy automatically when a certain event occurs,*

1. Select the required group in the results panel, and either select the **Properties** command from the context menu, or use the corresponding item in the **Action** menu.
2. Select the **General** tab In the application group policy configuration window **Properties: <Policy name>** (see Figure 37).
3. Check the **Activate policy based on the event** box and select the event you need from the drop-down list (for example, a virus attack).

To cancel automatic activation of the policy by event, the box must be unchecked.

4. Press the **Apply** or **OK** button.

If you deactivate policy by event, you can only return manually to the previous policy.

Following activation, a policy becomes effective based on the value selected in the **Advanced** window (cf. Figure 39).

### 3.1.1.6. Policy for mobile user

Such type of policy available only for Kaspersky Anti-Virus for Windows Workstations versions 5.0 and 6.0, and for Kaspersky Anti-Virus 5.0 for Windows File Servers and Kaspersky Anti-Virus 6.0 for Windows Servers.

*To configure the enforcement of a group policy when a client computer disconnects from the logical network,,*

1. Select the required group policy in the results pane, and either select the **Properties** command from the shortcut menu, or use the corresponding item from the **Action** menu.
2. Switch to the **General** tab (see Figure 37) in the **Properties: <Policy name>** application group policy settings window that will open.
3. Select the **Policy for a mobile user** item from the drop-down list in the **Policy status** field.
4. Press the **Apply** or **OK** button.

Following activation, a mobile user policy becomes effective based on the value selected in the **Advanced** window (cf. Figure 39).

### 3.1.1.7. Deleting a policy

*To delete a policy,*

select the required folder in the **Policies** folder of the results panel, and click the **Delete** command of the shortcut menu or in the **Action** menu.

### 3.1.1.8. Copying a policy

*To copy a policy,*

1. select the required folder in the **Policies** folder of the results panel and click the **Copy** command of the shortcut menu or in the **Action** menu.
2. Switch to the **Policy** folder of the new group (or stay in the same folder) and use the **Paste** command from the shortcut menu or from the **Action** menu.

As the result, the policy will be copied with all its settings and will be applied to the computers within the group into which it was copied. If a policy of the same name exists in the folder, the suffix `_1` will be automatically added to its name.

As the result of copying, the active policy becomes inactive. If required, you can make this policy active again (see section 3.1.1 on page 63).

### 3.1.1.9. Configuring the Network Agent's policy

When creating a policy for the Network Agent in the Settings window (see Figure 48), you can specify the following settings:

- in the **Event log** field, specify the maximum file size in the **Maximum size of event log**, **Mb** field.
- if you wish information about objects which have been quarantined or backed up on the computer to be automatically transferred to the Administration Server, check the corresponding boxes in the **Storages** field.
- press the **Modify** button in the **Network Agent uninstallation password** and enter the password. This password must be entered in the remote uninstallation task of the Network Agent.

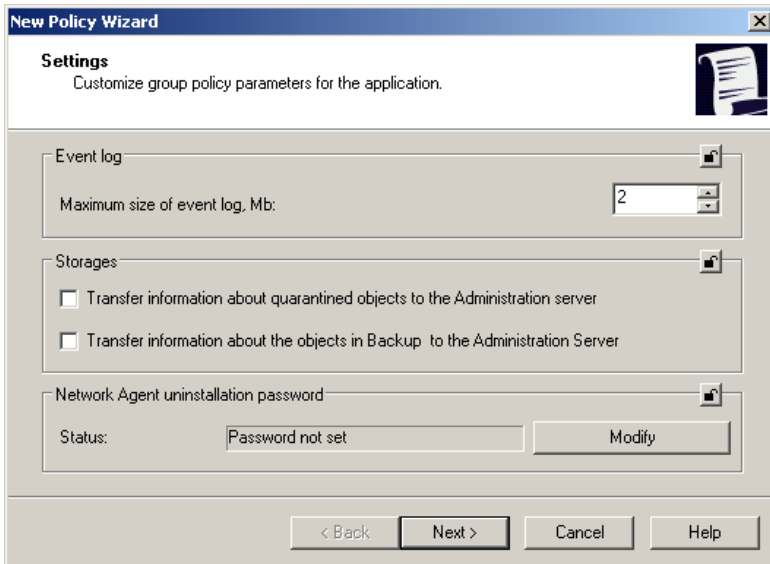


Figure 48. Creating policy for the Network Agent  
The **Settings** window

In the **Network** window (see Figure 49) you can specify the settings for connection to the Administration Server.

- Specify the following in the **Connect to the Administration Server** field:
  - in the **Synchronization period, min.** field specify the time interval (in minutes) between attempts to synchronize data of the client computers and the Administration Server.
  - check the **Use SSL connection** box if you wish the connection to be secure (using SSL protocol).
  - check the **Compress network traffic** box to increase the rate of the data transfer by the Network Agent, by decreasing the amount of the information transferred and hence decreasing the load on the Administration Server.

If you enable this setting, the load on the central processor of the client computer may be increased.

- In the **Network Agent port** field, allow the Administration Server connection to the client computers using a UDP port, and define the port number. To open the connection via the UDP port, check the **Use UDP port** and enter the port number in the **UDP port number** field. The default value is **15000**. Only decimal representation is allowed.

If the client computer is running Microsoft Windows XP Service Pack 2, the in-built firewall will block UDP port 15000. To access the Administration Server, you will have to open this port manually.

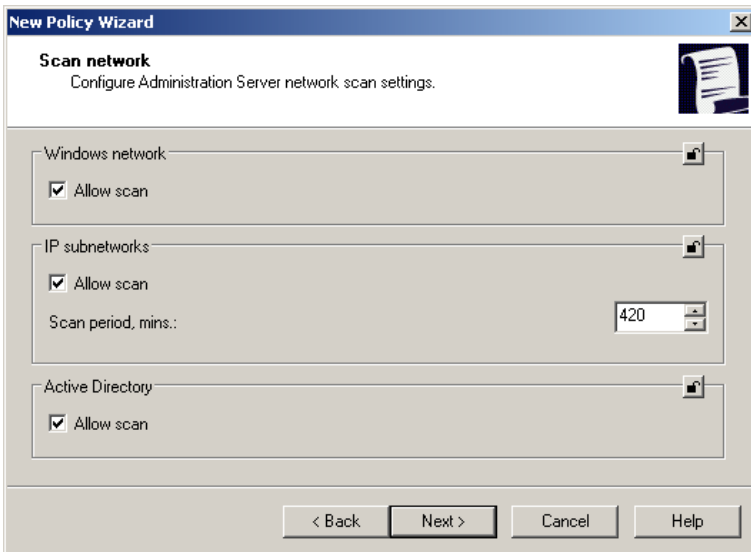


Figure 49. Creating policy for the Network Agent: The **Network** window

When editing the policy for the Network Agent, you can make changes on either the **Settings** tab (see Figure 50) or the **Network** tab (see Figure 51).

In addition to configuration through the policy wizard, the **Network** tab may also be used:

- Check **Allow NetBIOS name service in Anti-hacker for KAV 6.0 for Windows Workstations** . This will open UDP Port 137 which Kaspersky Antivirus 6.0 Anti-Hacker uses to obtain the Administration Server IP address.

- Check **Open Administration Agent Ports in Windows Firewall**. This will cause the UDP port required to support Administration Agent to be added to the Microsoft Windows firewall exception list.

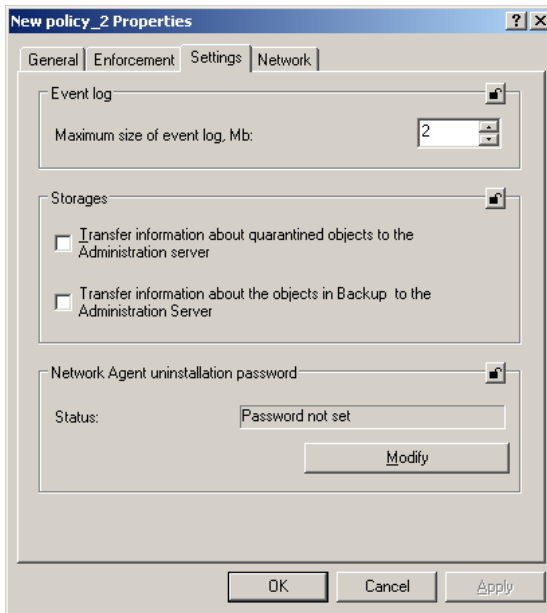


Figure 50. Creating policy for the Network Agent  
The **Settings** window

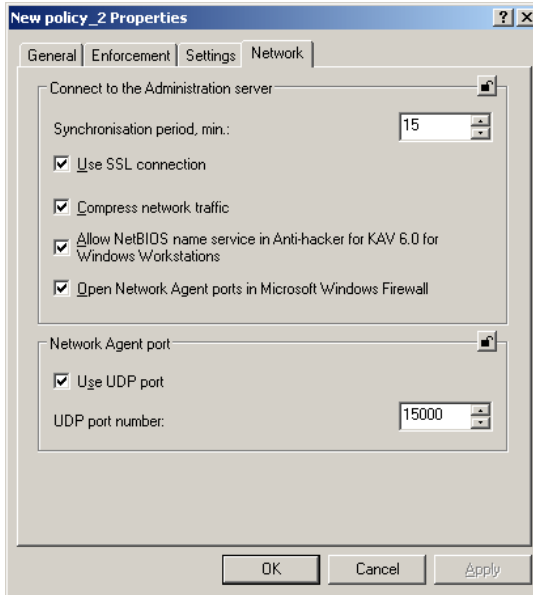


Figure 51. Creating policy for the Network Agent  
The **Network** window

### 3.1.1.10. Configuring the settings of the Administration Server policy

When creating a policy for the Administration Server, specify **Kaspersky Administration Kit** in the application selection window. Then, using the **Settings** window (see Figure 52), specify the following:

- In the **Connection settings for the Administration Server** field:
  - the number of the port used to connect to the Administration Server. The default value is **14000**. If this port is in use, it can be changed;
  - the number of the port to be used for secure connection to the Administration Server using SSL protocol. By default port **13000** will be used.
- Specify the required value in the **Maximum number of events stored in the database** field. The default value is 400,000 records.

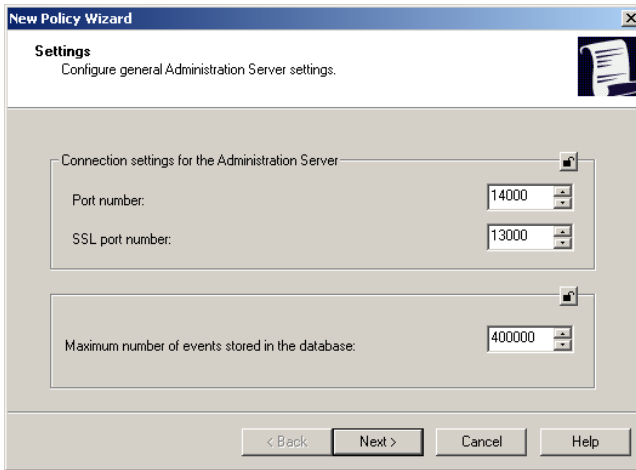


Figure 52. Creating policy for the Administration Server  
The **Settings** window

In the **Scan network** window (see Figure 53) you can specify how the the Administration Server updates its information about the Windows network structure.

- To enable automatic network polling, check the **Allow scan** box in the **Windows network** group.
- To enable automatic polling of IP subnetworks, check the **Allow scan** box in the **IP subnets** group. The Administration Server will poll subnetworks with the period specified in the **Scan period, min.** field. By default the interval between polls is 420 minutes.
- To allow automatic network polling using the Active Directory structure, check the **Allow scan** box in the **Active Directory** group.

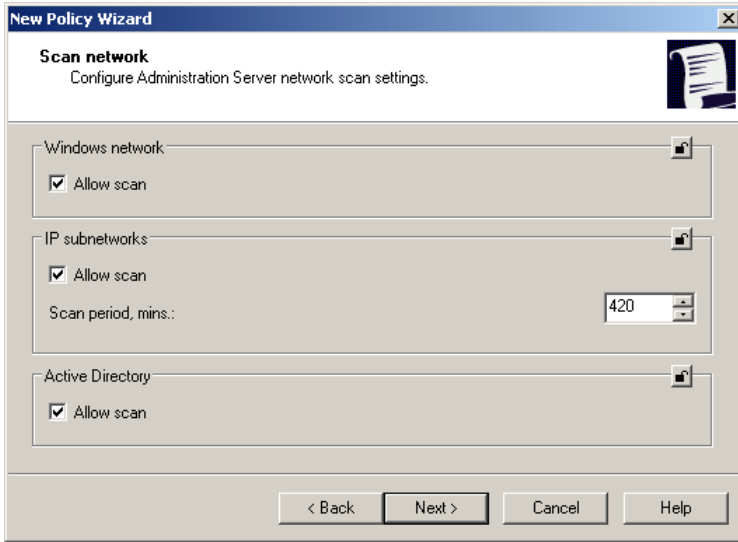


Figure 53. Creating policy for the Administration Server  
The **Scan network** window

In addition to values configured while a policy was being created, other policy parameters may be modified.

Use the **Host visibility time-out, mins:** field on the **Settings** tab to specify the time during which the client computer will be considered visible to the network after the connection with the Administration Server has been lost. The default value is 60 minutes. After the specified time elapses, the Administration Server will consider the client computer inactive.

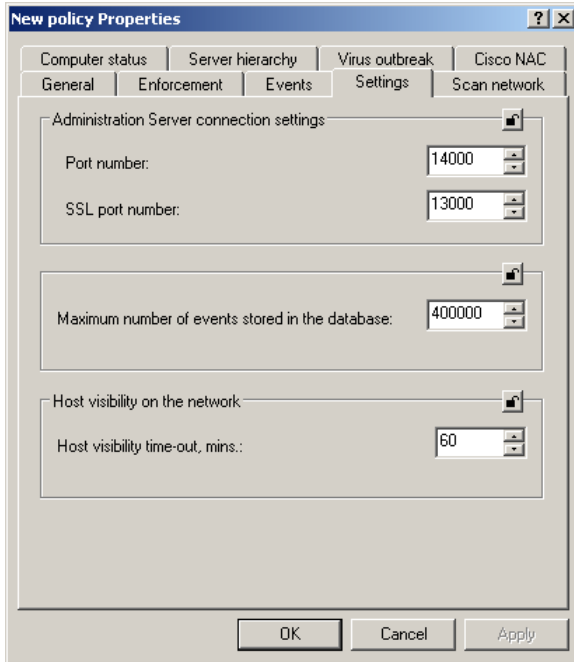


Figure 54. Editing policy for the Administration Server  
The **Settings** window

On Scan network tab (cm. Figure 55) you can specify:

- Windows network polling intervals:
  - **Full scan time, min.** additional information on computers is requested, including Operating System, IP address, and DNS name. The default polling frequency is 60 minutes.
  - **Quick scan time, mins.** only information on hosts in a list of NetBIOS names in all network domains and workgroups is collected. The default query frequency is 15 minutes.

- Active Directory polling intervals Administration Server queries the network with the frequency specified in **Scan period (mins.)**. The default polling frequency is 60 minutes.

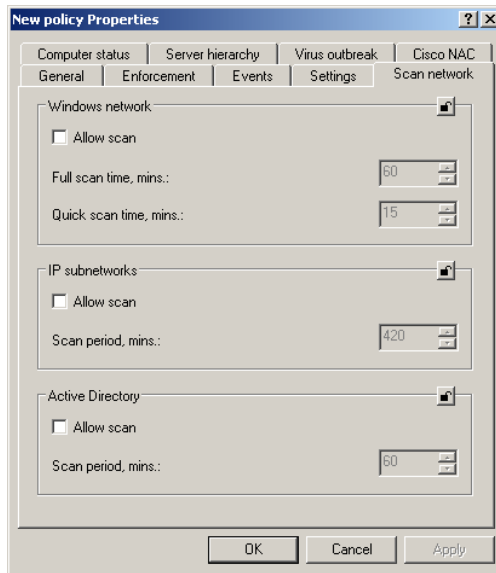


Figure 55. Administration Server policy settings  
**Scan network** tab

The **Virus Outbreak** tab is used to specify when the **Virus Outbreak** event will be raised for each antivirus application type. The settings on this tab are identical to those in the like-named tab under Administration Server properties.

The **Cisco NAC** tab may be used to define a mapping between antivirus protection conditions and Cisco NAC statuses. The settings in this tab are identical to those in the like-named tab under Administration Server properties (cf. Figure 72).

The **Administration Server Hierarchy** tab (cf. Figure 56) may be used to disable or enable the editing of hierarchy settings. If **Enable Editing of Hierarchy Settings on Slave Administration Servers** is unchecked, slave Administration Servers will not be able to modify hierarchy parameters set on the master Server.

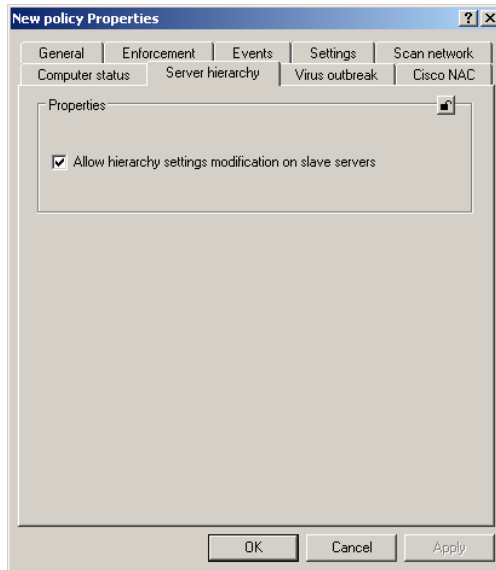


Figure 56. Editing Administration Server Policies  
**Server Hierarchy** Tab

### 3.1.1.11. Exporting policies

*To export a policy:*

In the console tree, select the required group and click the **Policies** folder. The results pane will display a list of all policies existing for this group. Select a policy, and click **Export** on the shortcut menu, or on the **Action** menu.

In the window that opens, specify the name of the file where the policy will be saved and its location. Click **Save**.

### 3.1.1.12. Importing policies

*To import a policy:*

In the console tree, select the required group. Open the shortcut menu of the **Policies** folder and click **All tasks/Import**. The same command can be accessed on the **Action** menu.

In the window that opens, specify the name of the file from which the policy will be imported and click **Open**.

## 3.1.2. Viewing application settings

### 3.1.2.1. Viewing application settings

*To view/configure application settings:*

1. Select the group in the **Groups** folder that includes the required client computer. In the details panel, select the computer on which the target application is installed. Click the **Properties** command on the shortcut menu or on the **Action** menu.
2. The **<Computer name> Properties** dialog box containing several tabs will appear in the main program. Switch to the **Applications** tab, which lists all Kaspersky Lab applications installed on this computer and displays general information about them. If the client computer is an administrator workstation and/or a Administration Server, the list contains the Kaspersky Administration Kit components (Network Agent and/or Administration Server).

Select the target application. You can:

- Click the **Events** button to see the list of application-related events that occurred on the client and were logged on the Administration Server.
- Clicking the **Statistics** button to see current statistics on the application's performance. The Administration Server requests this information from a client. If the connection is lost, a corresponding error message will be displayed.
- Clicking the **Properties** button in the "**<Application name>**" **application properties** dialog box to view general information about an application and configure its settings.

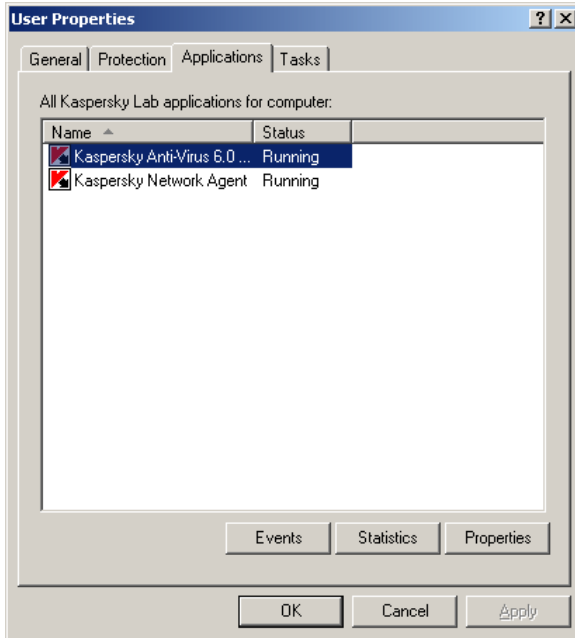


Figure 57. Client properties dialog box.  
The **Applications** tab

The **Application setting "<Application name>"** dialog box consists of several tabs, which show information updated during the last client/server synchronization. The tabs are specific to each application. For more information about the tabs, see the corresponding user documentation. The **General**, **Licenses**, and **Event processing** tabs are common for all applications.

On the **General** tab, you can view general information about the application, start/stop the application, and view settings of the plug-in for this application installed on the administrator workstation by clicking the **Plug-in information** hyperlink.

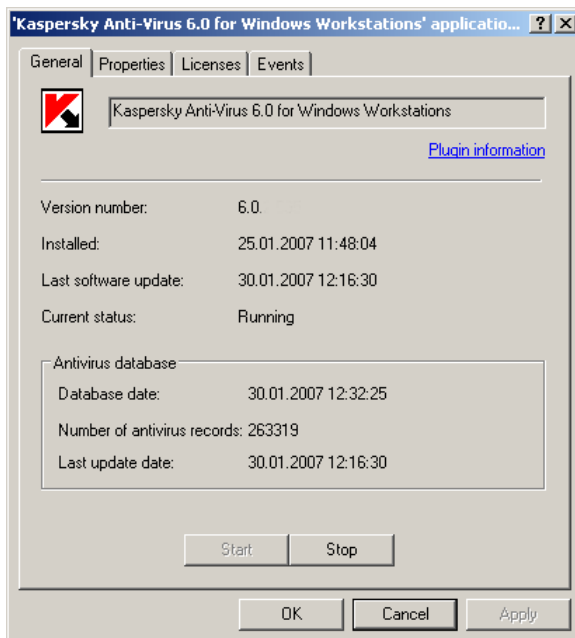


Figure 58. Application properties dialog box.  
The **General** tab

On the **Licenses** tab, you can view detailed information about the current and reserve license keys installed on a client computer.

In the **Current license key** field, you can view data on the current license key:

- **Number** - the license key serial number.
- **Type** – type of the installed key (for example, commercial or test)
- **Activation date** – key activation date
- **Expiration date** – expiration date for the license
- **License period** – license validity period
- **Limit computer count** – the license restrictions imposed by the key.

The **Reserve license key** field displays data on the next license key:

- **Serial number** - the license key serial number.
- **Type** – type of the reserve key (for example, commercial or test)
- **License period** – license validity period
- **Limit computer count** – the license restrictions imposed by the key.

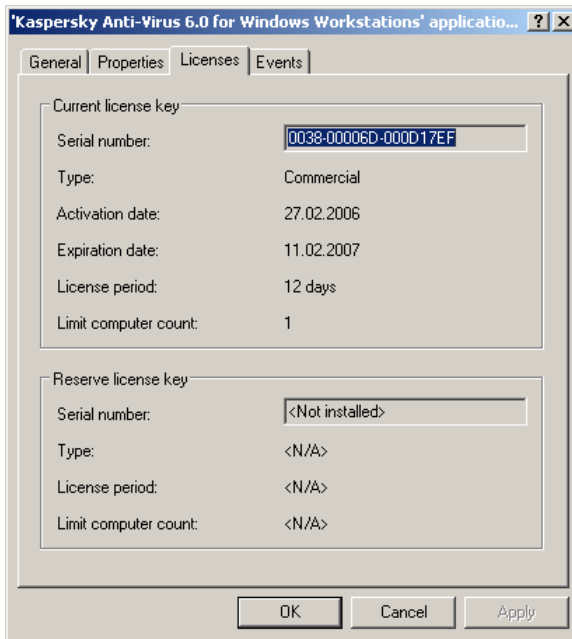


Figure 59. Application properties dialog box.  
The **Licenses** tab

The **Event severity** tab displays rules for handling events occurred on a client computer. You can view them and make necessary changes. This tab is identical to the **Event processing** tab of the **<Policy name> Properties** dialog box (details see section 3.1.1.2 on page 66).

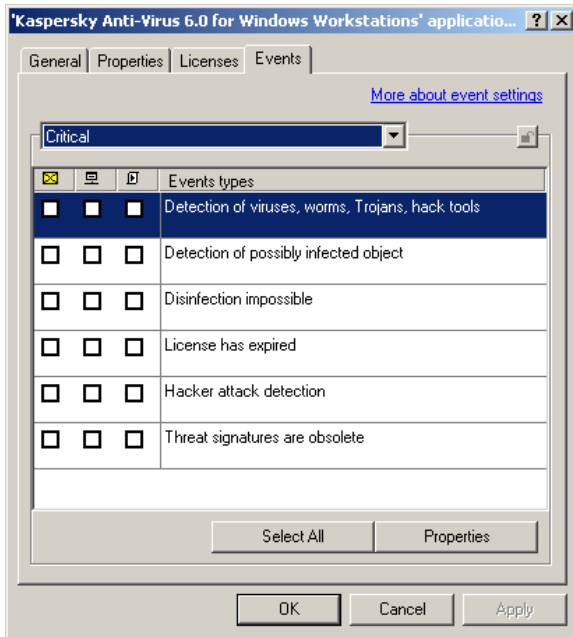


Figure 60. Application properties dialog box.  
The **Events** tab

- To confirm any changes, press the **Apply** or **OK** button.

### 3.1.2.2. Administration Server settings

To view the Administration Server settings:

in the console tree, select the **Kaspersky Administration Server (<Server name>)** node that corresponds to the required Administration Server. Click **Properties** either on the shortcut menu or in the **Action** menu.

This will open the **Kaspersky Administration Server (<Server name> Properties** dialog box that contains the **General**, **Settings**, **Event processing**, **Notification**, **Virus outbreak**, **Security** and **Scan network, CISCO NAS** tabs.

The following information is displayed in the **General** tab (see Figure 61):

- name of the Administration Server component and the computer name within the Windows network on which this component is installed;
- the version number of the installed application;
- path of the public access folder used for storing application deployment files and the updates downloaded to the Administration Server.

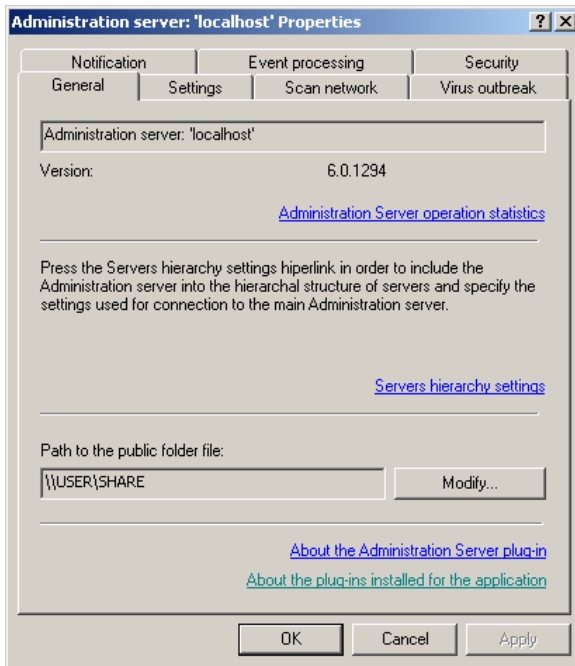


Figure 61. Viewing the Administration Server properties.  
The **General** tab

You can change the path to the public access folder using the **Browse** button.

The **Administration Server operation statistics** hyperlink is used to open the window which displays general statistics about the Administration Server.

Click the **About the Administration Server plug-in** hyperlink to view the plug-in's properties (see Figure 62). The following information is provided:

- Name and full path to the plug-in
- File version
- Name of the application that includes this plug-in (**Kaspersky Administration Kit**)
- Application version
- Information about the manufacturer (**Kaspersky Lab**) and copyright information
- Date and time of plug-in creation.

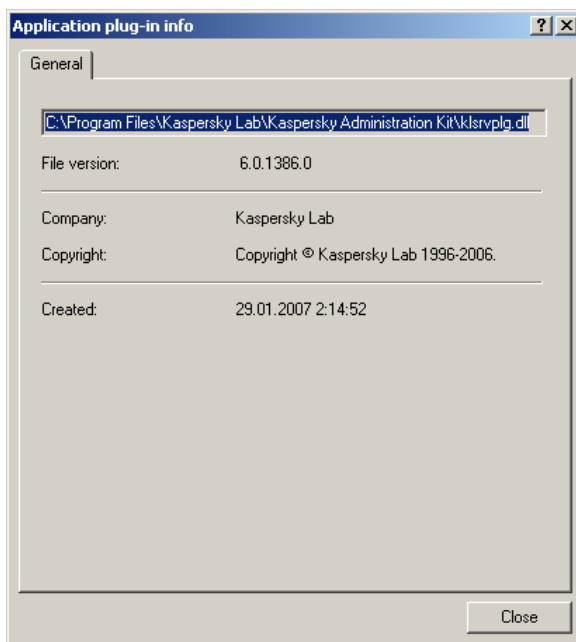


Figure 62. Viewing application plug-in properties.  
The **Application plug-in info** of the Administration Server

Using the **About the plug-ins installed for the application** link, you can open a window that contains the list of plugins installed on the Administration Server (see Figure 63). For each plugin the application name and plugin versions are provided. By pressing the **Information**

button in this window you can view detailed information about the selected application management plugin (see Figure 62).

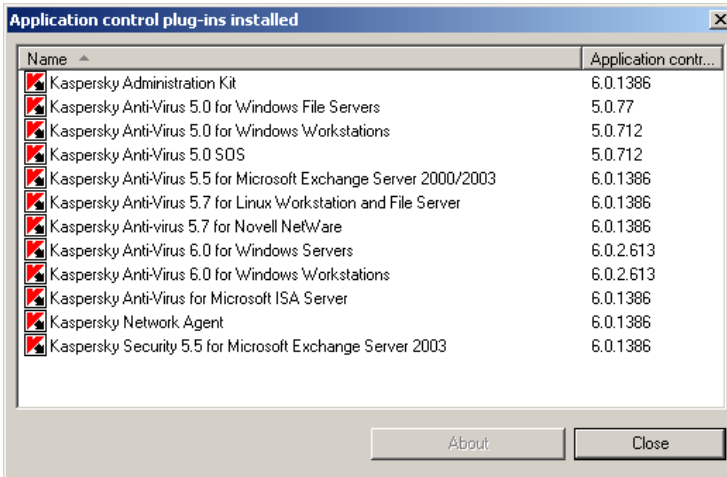


Figure 63. The list of application management plugins installed on the Administration Server

The tab also contains the **Master server settings** link that allows you to edit the properties of the selected slave server. In this dialog box, you can:

- Specify whether this Administration Server is a slave server
- Specify the address and port of the master Administration Server
- Specify or modify the path to the master Administration Server certificate
- Set proxy server parameters to connect to the master Administration Server (if necessary)

These parameters cannot be edited if **Enable Editing of Hierarchy Settings on Slave Administration Servers** is unchecked in the current Administration Server hierarchy (cf. Figure 56).

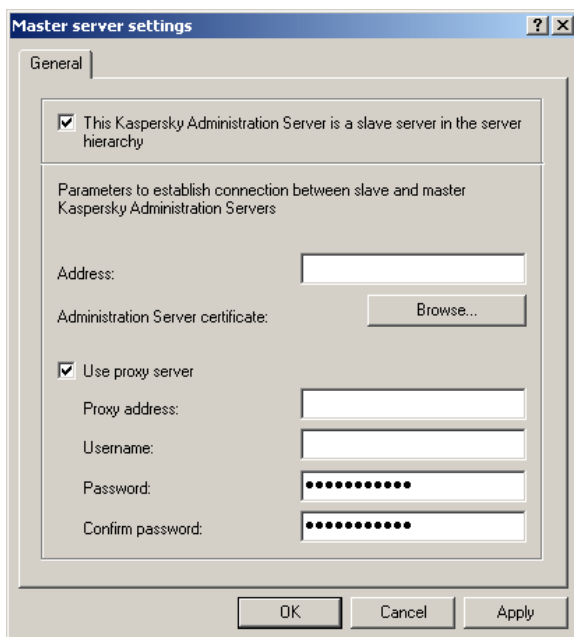


Figure 64. Properties of a slave Administration Server

The **Settings** tab shows Administration Server properties. The **Connection settings for the Administration Server** group has the following fields:

- **Port number** displays the port number used to connect to the Administration Server. The default port number is 14000. If this port is already in use, you can change it.
- **SSL port number** displays the SSL port number used to securely connect to the Administration Server. The default port is **13000**.
- Port number that will be used by mobile devices to connect to Administration Server. Port 13292 is used by default. To enable this port on Administration Server, check Open port for mobile devices.<sup>3</sup>

---

<sup>3</sup> A mobile device is defined as a device with Kaspersky Anti-Virus 6.0 Mobile Enterprise Edition installed.

Additionally, using the corresponding field you can specify the maximum number of events stored in the database on the Administration Server.

In the **Host visibility time-out, mins.** field of the **Host visibility on the network** group, you can specify the time during which a client computer will be considered visible in the network after it was disconnected from the Administration Server. The default value is 120 minutes. After the specified time has elapsed, the Administration Server will consider the client computer inactive.

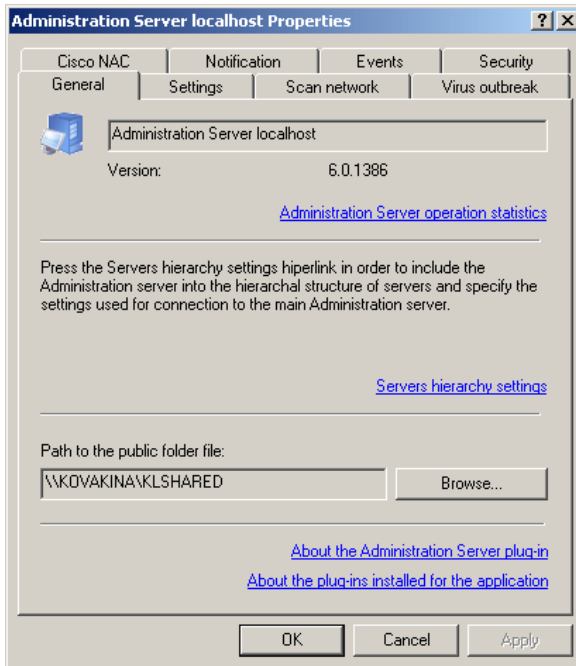


Figure 65. Viewing Administration Server properties.  
The **Settings** tab

The **Event processing** tab shows rules for handling events by the Administration Server. This tab is identical to the **Event Processing** tab in the Group policy properties dialog box (see section 3.1.1.2 on page 66).

Below we describe server events in more detail. For the Administration Server, as well as for other Kaspersky Lab applications managed through

Kaspersky Administration Kit, events fall into one of the four severity levels: **Critical**, **Error**, **Warning**, and **Info**.

The list below shows events included in each severity level:

- **Critical** events:
  - The license restriction for this license key has been exceeded. For example, the client computer on which the license key is installed, exceeds the restriction on the number of computers imposed by this key.
  - **Virus outbreak!** – virus activity exceeds the preset limit.

The response of the Administration Server to the **Virus outbreak!** event is extremely important, especially when a virus outbreak occurs and the risk of virus attacks increases.
  - **Host is out of control** – unable to establish connection with the Network Agent installed on the client computer.
  - **Host status is 'Critical'** - a computer with settings matching the **Critical** status has been detected within the network.
- **Error**:
  - **There is no space on the disk** – there is no free space on the disk where the Administration Server saves operational information.
  - **The shared folder is unavailable** – the shared folder containing database and module updates is unavailable.
  - **The Administration Server database is unavailable** – the server database is inaccessible.
  - **The Administration Server database is full** – there is no space in the server database.
- **Warning**:
  - The license restriction for this license key has been exceeded.
  - The client computer has been invisible on the Windows network for a long time.

- **Host names conflict** – the uniqueness of client names within one hierarchical level is violated.
- **Volumes are almost full** – little or no free space is left on the hard drives.
- Insufficient space in the information database of the Administration Server.
- Connection with the main Administration Server has been lost.
- Connection with the slave Administration Server has been lost.
- **Host status is 'Warning'** - a computer with the **Warning** status has been detected on the network.
- **Info:**
  - License restriction - the number of licenses in use is over 90% of the maximum number supported by this license key.
  - **New host found** – a new client has been found during network browsing.
  - **The host was automatically added to group** – a new client has been automatically included in a group in accordance with the Unassigned node settings.
  - **This computer has been inactive for too long and is removed from the group** – a client computer did not respond for a long time and was removed from the logical network.
  - Connection with a slave Administration Server has been established.
  - Connection with a master Administration Server has been established.
  - Audit: Connection to the Administration Server.
  - Audit: Object change.
  - Audit: Object status change.
  - Audit: Group parameters change.

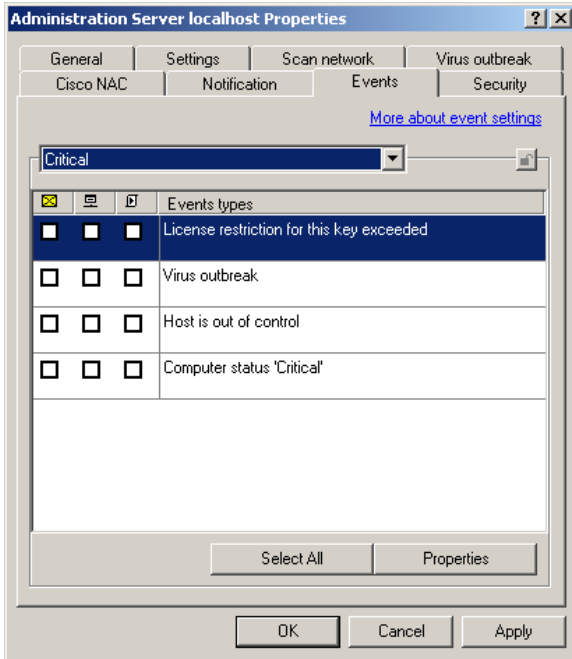


Figure 66. Viewing Administration Server properties.  
The **Event processing** tab

On the **Notification** tab, you can set parameters for notifying the administrator and / or other users on events sent to the Administration Server from anti-virus applications. These settings are used by policies for applications as default settings. Settings on this tab match the policy settings. Specify:

- email notification parameters:
  - Enter the notification recipient's e-mail address in the **Recipient Address** field. You can use multiple addresses, in a list separated by commas or semi-colons;
  - Enter the mail server address in the **SMTP Server Address** field. An IP address or a Windows network name may be used;
  - Specify the SMTP server port number in the **SMTP Server Port Number** field. The default value is 25;

- **Computers for NET SEND Notification:** specify destination addresses for network notification recipients. An IP address or a Windows network name may be used. Multiple addresses may be entered as a list separated by commas or semicolons.

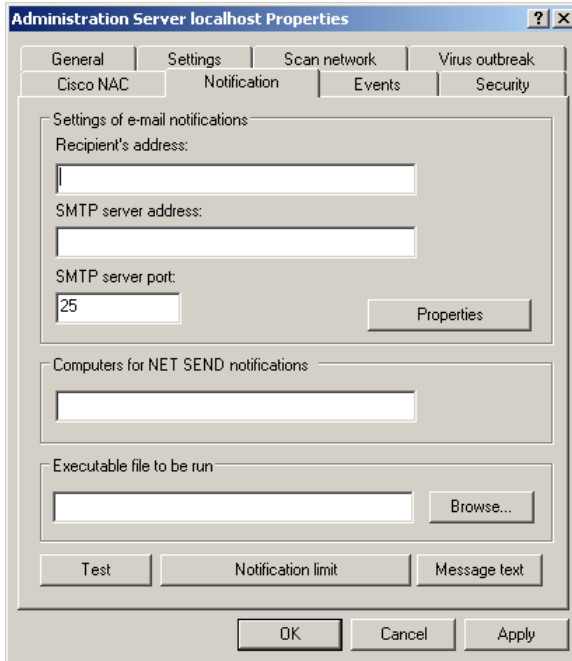


Figure 67. Viewing Administration Server properties.  
The **Notification** tab

- **Run Executable** group: use the **Browse** button to select an executable to run when an event is triggered.

Executable environment variable names are the same as the names of the substitute parameters used to create the message text (see below).

- Enter the text of the notification message. Click the **Message** button, and create a template in the resulting window (cf. Figure 68).

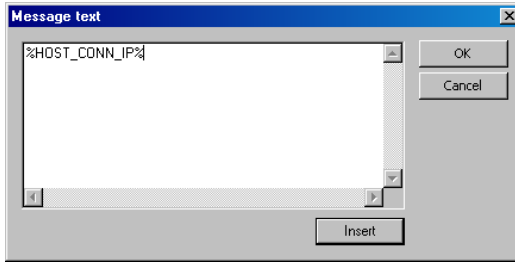



Figure 68. Configuring notification Message Entry

A message may include information on a logged event. This requires that appropriate placeholders be placed in the template by selecting from a drop down list accessible through the  button.

- sender and subject line for notification message. Click the **Options** button and configure appropriate values in the resulting window (cf. Figure 43).

To reduce the impact on the Server's resource usage, limit the number of notifications sent by the Administration Server by clicking the **Notification restrictions...** button. In the window that will open (see Figure 69), check the **Limit notifications** box and specify the following criteria:

- maximum number of notifications sent by the Administration Server.
- time period during which the Administration Server can generate the notifications.

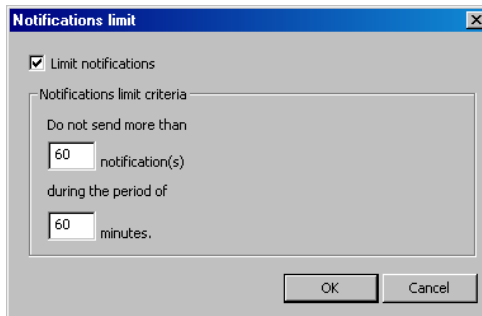


Figure 69. Limiting the number of notifications

These are default policy settings used in Kaspersky Lab's applications.

To check the correctness of the settings specified on this tab, you can send a text message by clicking the **Test** button. This will open a test notification sending window. If any errors occur, detailed information about them will be displayed.

On the **Virus outbreaks** tab (see Figure 70) you can set the **Virus outbreak event generation criteria**, which specify the maximum number of detected viruses during a specified time interval. If the number of viruses detected for a short period exceeds the threshold, the event is classified as a **Virus outbreak**. This parameter allows the administrator to prepare and respond to a virus outbreak.

*Check the desired application types:*

- **Antivirus for workstations and file servers;**
- **Antivirus for perimeter defense;**
- **Antivirus for mail systems.**

*Set the virus activity threshold for each application type which when exceeded will trigger a **Virus Outbreak** event:*

- **Viruses** field: number of viruses detected *by this type of application in the logical network;*
- **In (minutes)** field: *time during which the specified number of viruses were detected.*

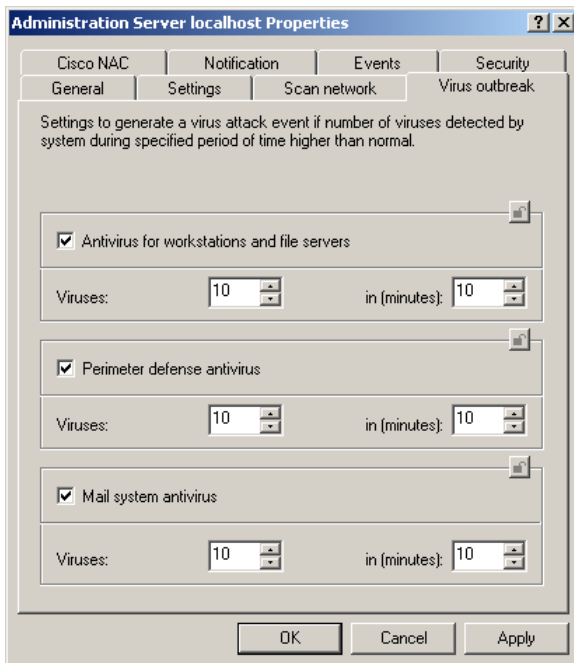


Figure 70. Viewing Administration Server properties.  
The **Virus outbreaks** tab

The **Security** tab (see Figure 4) is used to configure the right to access the logical Administration Server logical network (see section 2.2.1 on page 16).

The Network polling tab (see Figure 67) displays the settings of the computer network polling by the Administration Server.

The **Windows network** group of fields is used to configure the general network polling settings. To enable automatic network polling, check the **Allow scan** box. Specify in the fields below:

- **Quick scan time, mins.** Information about the list of NetBIOS names of computers in all network domains and workgroups will be updated with the specified frequency. By default the polling interval is 15 minutes.
- **Full scan time, mins.** Complete information about computers in the network, including operating system, IP address, and

DNS name, will be updated with the specified interval. By default the polling interval is 60 minutes.

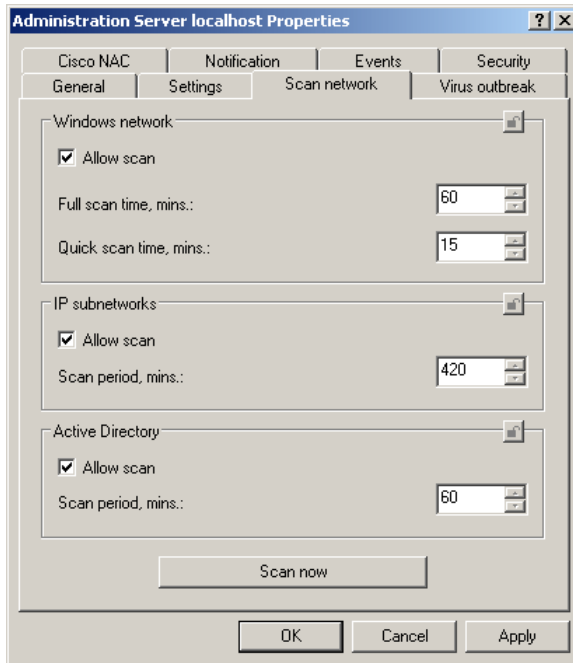


Figure 71. Viewing the Administration Server properties.  
The **Scan network** tab

The **IP subnets** group of fields contains settings that define IP polling. If the **Allow scan** box is checked, the Administration Server will poll the specified IP ranges using ICMP packets, and collect a complete set of data on hosts within the range. Polls occur with the frequency specified in the **Scan period, mins.** field. By default the polling interval is 420 minutes. You can specify a different value, or cancel polling by unchecking the **Allow scan** box.

The **Active Directory** group of field box contains settings that define network polling based on Active Directory unit structure. This causes information on Active Directory unit structure and host DNS names to be entered into the Administration Server database. If the **Allow scan** box is checked, the Administration Server will poll the network with the frequency specified in the **Scan period, mins.** field. By default the polling

interval is 60 minutes. You can specify a different interval, or cancel the polling by unchecking the **Allow scan** box.

To manually start full computer network polling, press the **Scan now** button.

The **Cisco NAC** tab (cf. Figure 72) contains parameters required for the integration of Kaspersky Administration Kit and Cisco Network Admission Control (NAC). This provides a mapping between client antivirus protection conditions and Cisco NAC statuses.

When integrated with Cisco NAC, the Administration Server acts as a standard Posture Validation Server (PVS) component, which an administrator may use to either allow a computer to access, or prevent it accessing, the network, depending on antivirus protection condition.

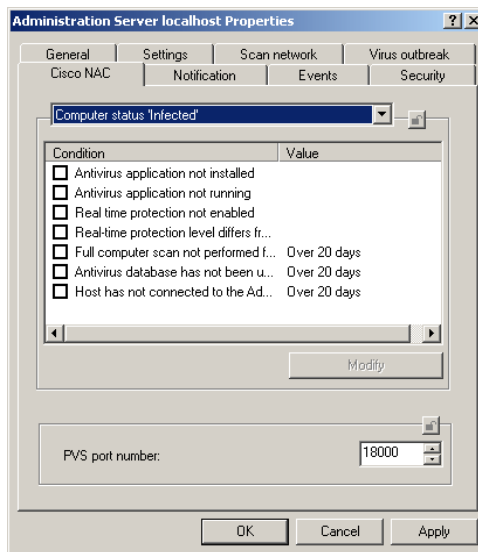


Figure 72. Viewing Administration Server Properties.  
**Cisco NAC Tab**

The upper field is used to select a Cisco NAC status: **Healthy**, **Checkup**, **Quarantine**, or **Infected**. The table below contains antivirus protection conditions which are mapped to the above statuses using checkboxes. Threshold values may be modified for some conditions. Select a condition in the **Condition** column and use the **Edit** button to open an editing

window (cf. Figure 73). Set the desired parameters in this window's **Value** field.

Set the Posture Validation Server port used to exchange data with the Cisco server in the **PVS Port Number** field. The default port is 18000.

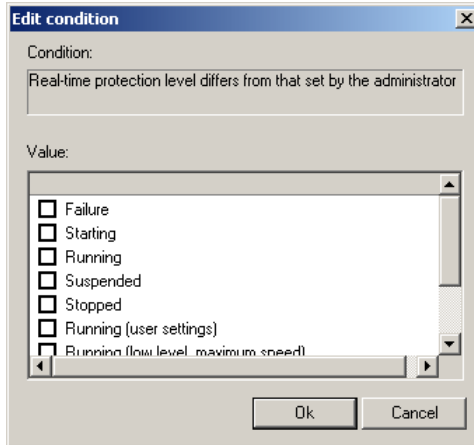


Figure 73. Editing Computer Antivirus Protection Status Selection Conditions

### 3.1.2.3. Configuring Network Agent

*To view the settings of the Network Agent installed on the client computer:*

1. Select the client computer in the results pane, and select the **Properties** command on the shortcut menu, or use the analogous item from the **Action** menu.
2. Switch to the **Applications** tab in the window that opens.
3. In the list of applications installed on the client computer, select **Network Agent** and press the **Properties** button.

When you are configuring Network Agent, in addition to the **General** and **Event processing** tabs, the **Kaspersky Network Agent application settings** window has the **Settings** (see Figure 76) and the **Network** (see Figure 77) tabs. The options displayed on these tabs are identical to those on the **Settings** and the **Network** tabs of the Network Agent policy settings dialog box (see section 3.1.1.9 on page 81).

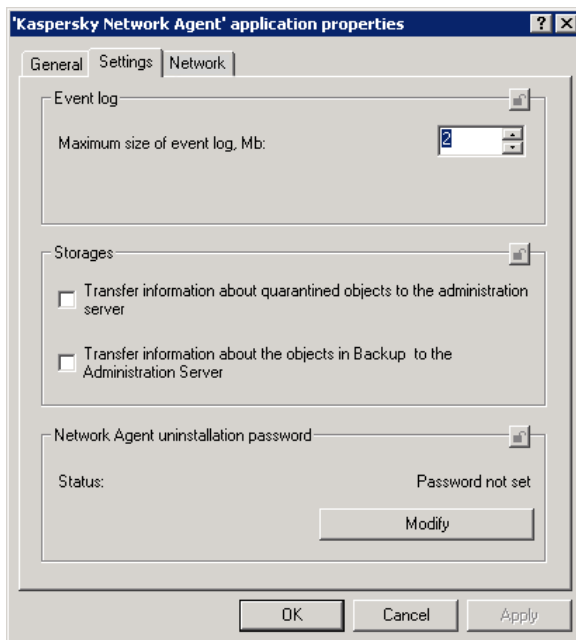


Figure 74. The Network Agent settings window  
The **Settings** tab

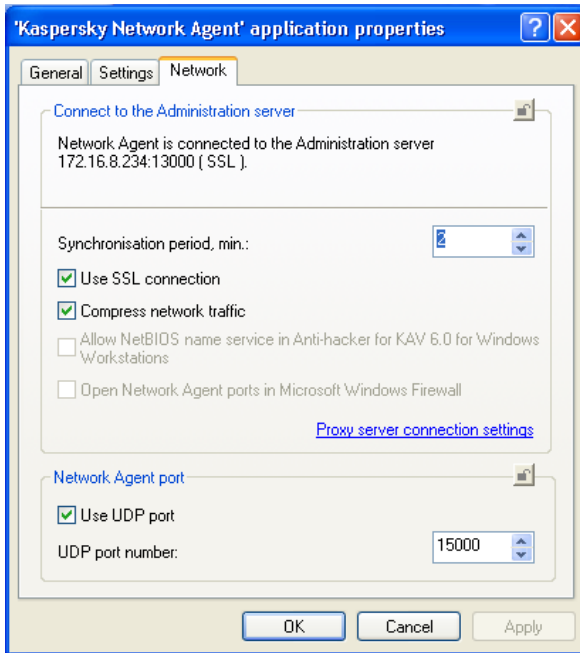


Figure 75. . The Network Agent settings window  
The **Network** tab

The Network Agent installed on the Server's computer can access only the **Settings** tab (see Figure 74). You do not have to configure settings for connecting the Agent to the Administration Server: these settings are hardwired which is possible because these components are installed on the same computer.

## 3.2. Managing applications' operation

### 3.2.1. Creating a group task

*To specify a new group task:*

1. In the console tree, choose the group for which you want to create the task and select the **Tasks** folder in this Group. On the shortcut

menu or the **Action** menu, click **New/Task** to start the new task wizard. Follow its instructions.

2. Specify the task name. If a task with this name already exists in the group, the **\_1** suffix will be added automatically to the new task name.
3. Select the application for which you want to create a task, and define the task type (Figure 76).

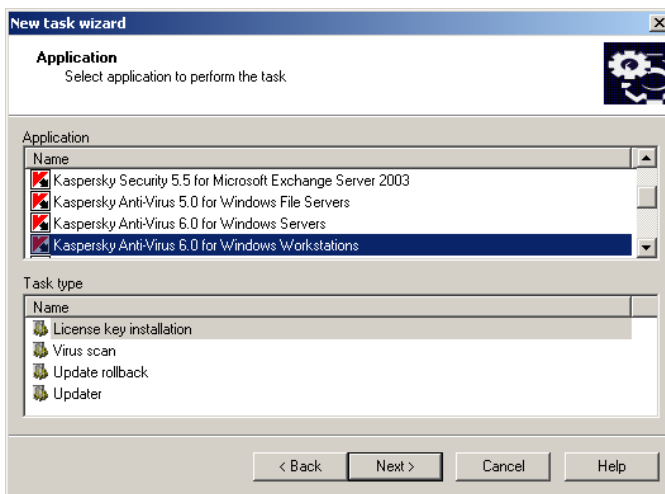


Figure 76. Creating a task. Selecting an application and defining task type

Select an application from the list, which displays all Kaspersky Lab applications that have Console Plug-ins installed on the administrator workstation. Select the type of the task from the **Choose type of task for execution** list, which lists the available tasks for the selected application.

If you are creating a report distribution task, choose **Kaspersky Administration Kit** as the application and **Report Distribution** as the task type (for details see the **Implementation Guide**).

4. You will then be prompted to configure the task according to the selected application (Figure 77). Some settings are set by default. For details about task configuration, see the documentation for a specific application.

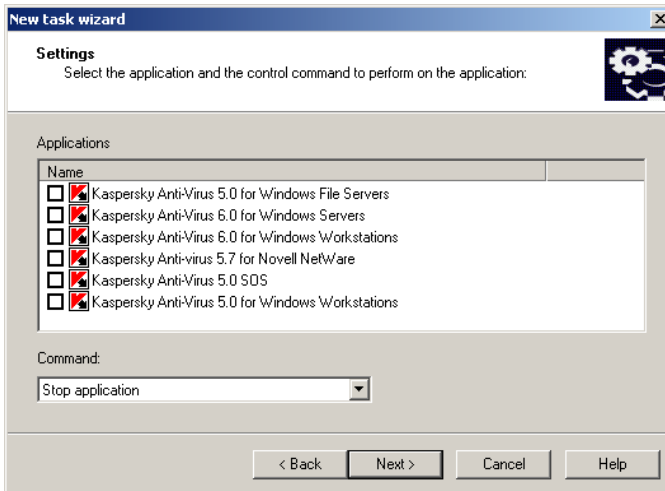


Figure 77. Task Configuration

5. Set a frequency and time of task startups.
  - In the **Schedule for** drop-down list, set the task to start:
    - **Every N hours;**
    - **Daily;**
    - **Weekly;**
    - **Monthly;**
    - **Once;**
    - **At application start** - start the task at application startup.
    - **Manually** – start the task manually from the Kaspersky Administration Kit main window, by clicking the **Start** command on the shortcut menu or on the **Action** menu.
    - **Immediately** – start the task immediately after the wizard finishes.
    - **On Receipt of Updates by Administration Server** - start the task automatically after updates are uploaded to Administration Server.
    - **On Completion of Another Task.**

- o **On Virus Outbreak Detection.**

|   |
|---|
| It is the list of all scheduling settings available. The list of available settings may vary depending on task type |
|---|

|   |
|---|
| Task for applications, which can be managed via Kaspersky Administration Kit only, can have extra schedule options. More information about it you can find in corresponding application's manual. |
|---|

- Specify schedule options in the fields specific to the selected schedule.

If you set up the task to start **Every N hours** (see Figure 78), specify the following:

- o The task start frequency in the **Every...** field and the start date and time for the task in the **Schedule to run** field.

For example, if you entered value 2 in the **Every...** field and entered August 3, 2006 15:00:00 in the **Schedule to run** field, the task will start every two hours starting at 15:00 on August 3, 2006.

The default frequency value is set at 6, and the default start date and time for the task is set to the current system date and time of your computer.

- o The procedure for the task to start if the client computer is unavailable (turned off, disconnected from the network, etc.) or if the application is not open at the time specified by the schedule.

Check the **Run missed tasks** box to make the system attempt to start a task next time the application is opened on this client computer. Tasks will be started immediately following a host's registering with the network if the task's schedule option is set to **Manually**, **Once**, or **Immediately**.

If this box **is** not checked (default), tasks on the client computers only scheduled tasks will be started, and for **Manually**, **Once**, and **Immediately** on hosts visible on the network only.

- o A variation of the scheduled time during which the task will be started on the client computers. This ability is provided to spread the load caused by simultaneous calls made to the Administration Server by numerous client computers when the task is launched.

Check the **Randomize the task start time within interval (min.)** box and specify time (in minutes) so that the client computers call the Administration Server during a certain time interval after the task is started, rather than simultaneously.

By default this box is unchecked.

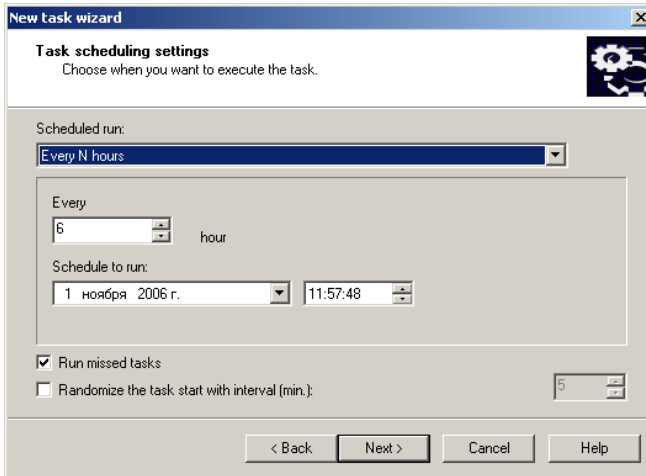


Figure 78. Scheduling a task to start **Every N hours**

If you set up the task to start **Daily** (Figure 79), specify the following:

- o The frequency of task startups in the **Every...** field and the start time in the **Schedule to run** field.

For example, if the **Every days** field has a value of 2 and the **Schedule to run** field has 15:00:00, the task will start once every two days at 3 p.m.

The default value for the **Every days** field is 2 and the current system time is the default task start time.

- o For instructions on what to do if a client is temporarily unavailable, see above.
- o About the randomized schedule option, see above

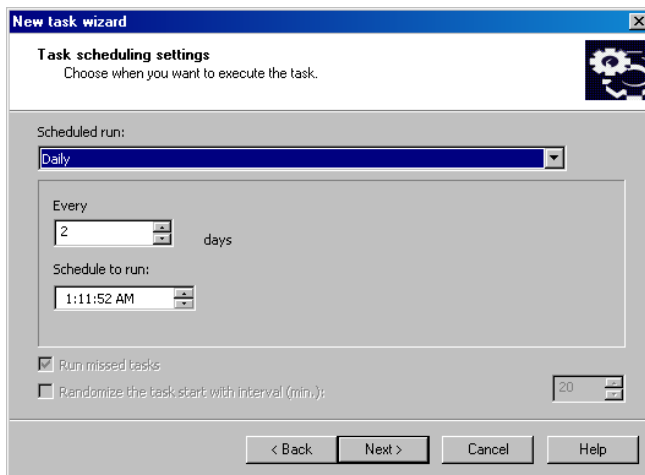


Figure 79. Scheduling a task to start **daily**

If you set up the task to start **Weekly** (Figure 80) specify the following:

- The frequency of task startups in the **Every** field and the start time in the **Schedule to run** field. By default, the task will start on Sunday, 18:00:00. You can change the default time, if necessary.

For example, if the value of the **Every** field is **Sunday** and the value of the **Schedule to run** field is 3:00:00 AM, the task will start every **Sunday** at 3 AM.

- For instructions on what to do if a client is temporarily unavailable, see above.
- About the randomized schedule option, see above.

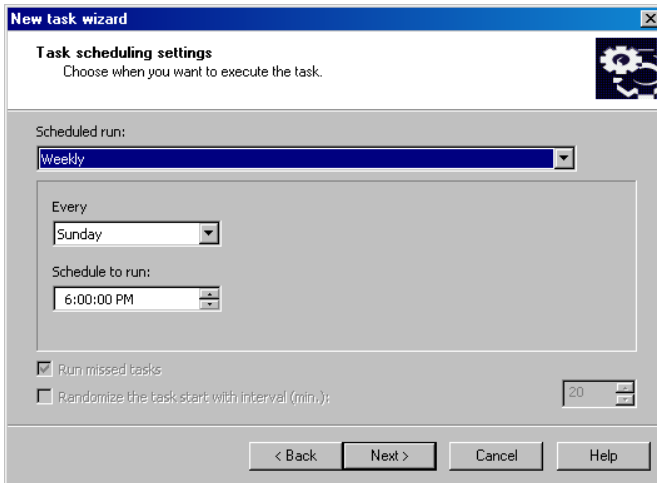


Figure 80. Scheduling a task to start every week

If you set up the task to start **Monthly** (Figure 81), specify the following:

- The frequency of task starting by selecting the date and time to start the task.

For example, if the value of the **Every... day of month** field is **20** and the value of the **Schedule to run** field is 3:00:00 AM, the task will start on the 20th of every month at 3 p.m.

The default value in the **Every... day of month** field is **1** and the current system time is set in the **Schedule to run** field.

- For instructions on what to do if a client is temporarily unavailable, see above.
- About the randomized schedule option, see above.

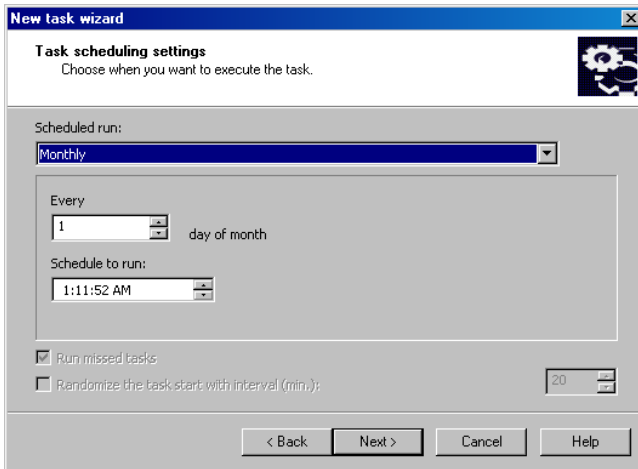


Figure 81. Scheduling a task to start every month

If you set the task to start **Once** (Figure 82), specify the following:

- The date of the task launch in the **Run on** field and the launch time in the **Schedule to run** field. The values of these fields are set automatically and correspond to the current system date and time. You can change them if necessary.
- For instructions on what to do if a client is temporarily unavailable, see above.
- For more on the randomized schedule option, see above.

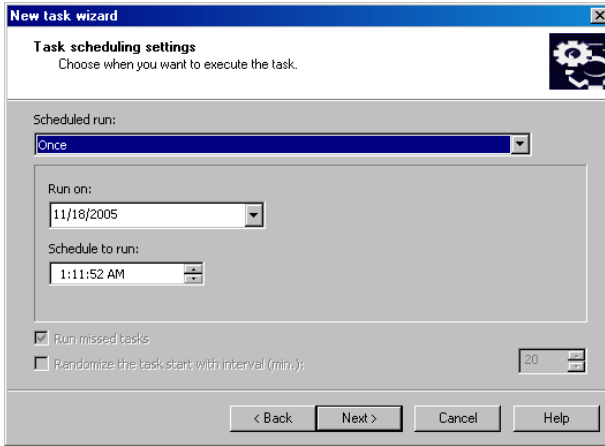


Figure 82. Scheduling a task to start once

If you set the task to start **Manually** (Figure 83), **At application start** or **Immediately after a task is created**, specify:

- Actions to take if a client is temporarily unavailable at task start (cf. description above).
- Randomized schedule for task to run on clients (cf. description above).

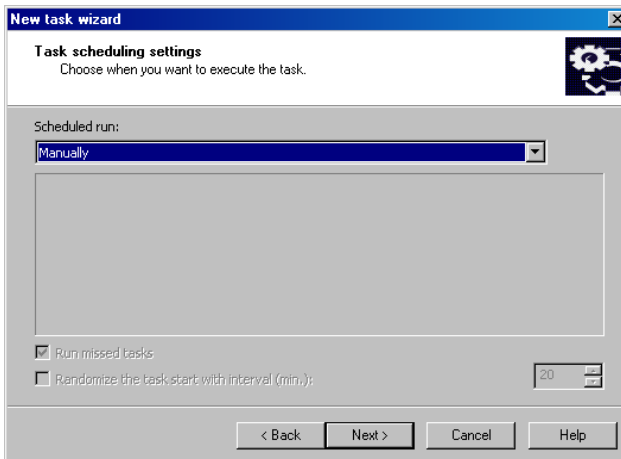


Figure 83. Setting a task to start manually

If you define that a task will start after another task completes, (cf. Figure 84), specify:

- The task after which the current task is to start. Select the desired task in the **Task Name** field using the **Browse** button. Specify exit status for the selected task in the **Exit Code** field: **Completed Successfully** or **Error**.
- Actions to take if a client is temporarily unavailable at task start (see above).

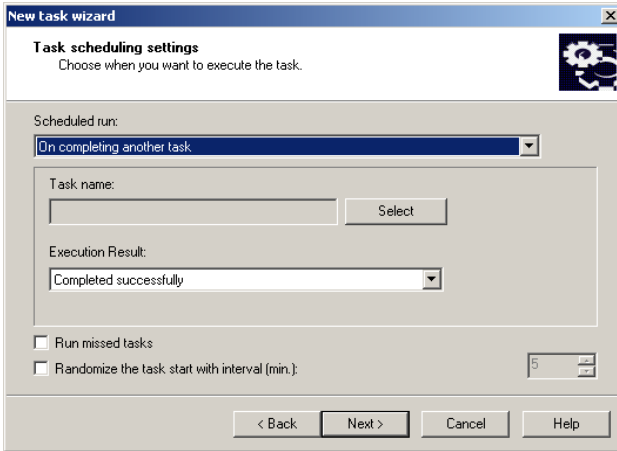


Figure 84. Task start following completion of another task

If a task is expected to start if a virus outbreak is discovered (see Figure 85), specify:

- Application types for which the **Virus Outbreak** event can start a task. Check the desired application types.
- Actions to take if a client is temporarily unavailable at task start (see above).

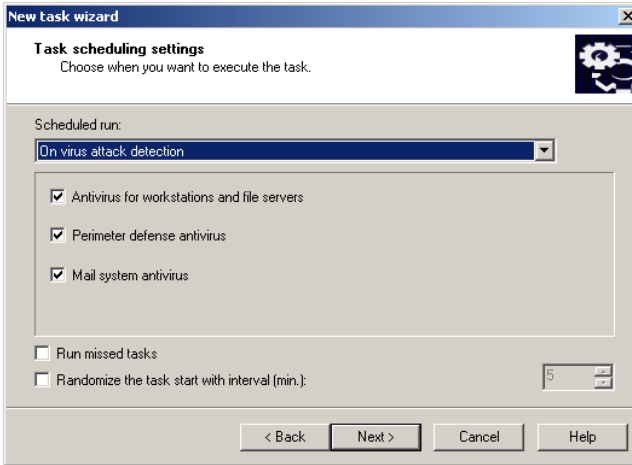


Figure 85. Task triggering by virus outbreak detection

After you finish with the wizard, the task you created will be added to the **Tasks** folders of the corresponding group and all nested groups, and displayed in the details panel. If necessary, you can configure task settings (see section 3.2.4 on page 124).

## 3.2.2. Creating a global task

*To create a global task:*

In the console tree, select the **Tasks** node and click the **New/Task** command on the shortcut menu or on the **Action** menu to start the new task wizard.

This wizard is similar to the wizard for creating group tasks. It has one additional stage when you should select clients from the logical network for which you want to create a task (Figure 86).

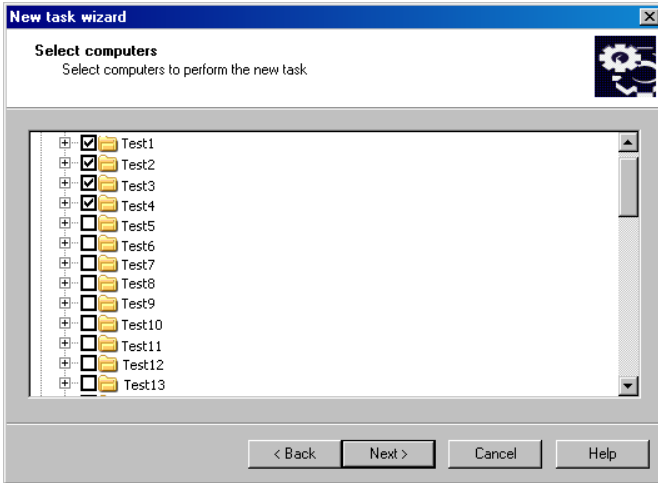


Figure 86. Creating a global task.  
Defining clients on which this task will be executed

Select logical network clients for which you want to create the task. You can select either computers from different folders or all computers in the current folder.

Global tasks will be executed only on specified clients. If new client computers are added to the group you selected, the task will not be performed for them. You should either create a new task or make appropriate changes to the current task settings.

After the wizard completes, the global task you created will be added to the **Tasks** node in the console tree and displayed in the details panel. With global tasks, you can perform all the operations available for group tasks.

### 3.2.3. Creating a local task

*To create a local task for a client computer:*

1. In the **Groups** folder, select the group that includes the target client computer. In the details panel, select the client for which you want to change application settings, and click the **Properties** item either on the shortcut menu or on the **Action** menu. After this, the

<Computer name> **Properties** dialog box will appear in the application main window (Figure 20).

2. Switch to the **Tasks** tab (Figure 87), which shows all tasks created for this client. To create a new local task, click **Add**. To configure task settings, click **Properties**.

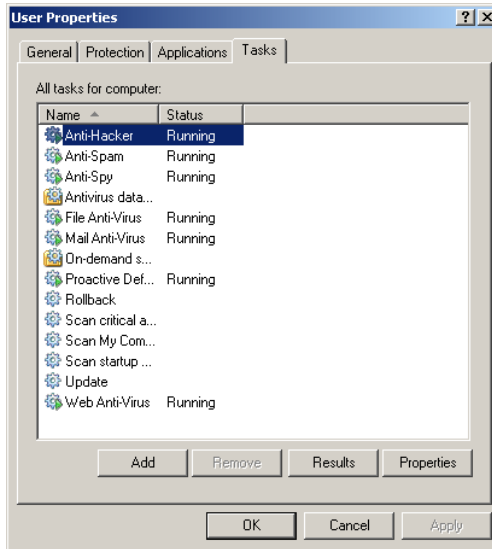


Figure 87. Creating a local task. The **Tasks** tab

For instructions on how to create and configure a local task, see the documentation for the corresponding applications.

### 3.2.4. Viewing and changing task settings

*To view and/or change task settings:*

- to create/modify a group task, choose a target group in the console tree and select the **Group Tasks** folder in this group. In the details panel, you will see all tasks assigned to this group. Select the required task, and choose the **Properties** item from the shortcut menu or from the **Action** menu.
- to change global task properties, choose the **Global Tasks** node in the console tree, select the task in the details panel, and click the **Properties** item on the shortcut menu or on the **Action** menu.

You will see the **<Task name> Properties** dialog box with the following tabs: **General**, **Properties**, **Account**, **Schedule**, and **Notification**. The global task property dialog box also has the **Target computers** tab.

The **<Task name> Properties** dialog box shows either the default settings for a task of this type or the last modified settings. The group policy settings for global tasks are not shown.

You can view the actual settings for this task in the **<Computer name> Properties** dialog box on the **Tasks** tab (Figure 87).

The **General** tab (Figure 88) displays general information about the task:

- Task name, which you can change if necessary
- Application for which the task was created (for example, Kaspersky Anti-Virus 5.0 for Windows Workstations)
- Application version
- Task type
- Task creation date and time
- Last command used manually (**Start**, **Stop**, **Pause**, **Resume**).

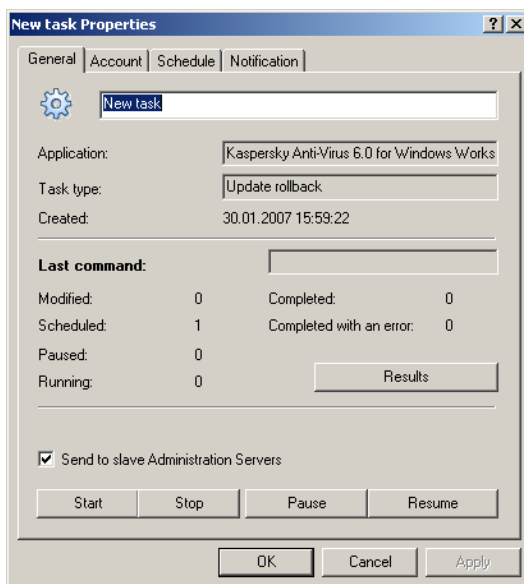


Figure 88. Editing task settings. The **General** tab

If a global task is set for these computers, the bottom of this tab shows statistics about the results of task execution on the client computers in this group. To view the details of task performance, click **History** (see section 3.2.16 on page 137).

On this tab, you can use the following buttons to manage the task manually: **Start, Stop, Pause, and Resume**.

You can temporarily remove the task from the list of scheduled tasks. To do this, uncheck the **Run at Scheduled Time** checkbox. Though the task will not be deleted, it will not be launched unless the **Run at Scheduled Time** checkbox is checked.

To copy the task on the slave Servers, check the **Distribute to the slave Administration servers** box.

The **Properties** tab (Figure 89) displays task settings specific to each application. For information about this tab, refer to the corresponding documentation.

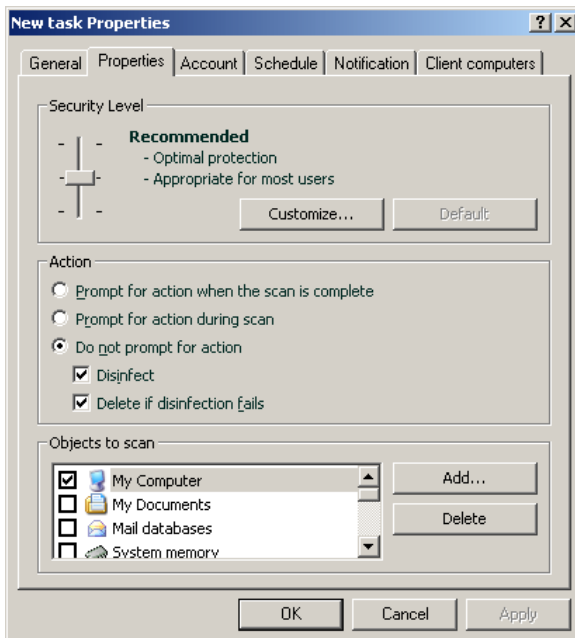


Figure 89. Editing task settings. The **Properties** tab

On the **Account** tab (Figure 90), you can specify the account under which the task will run:

- **Default account.** The task will run under the account of the application that will perform this task.
- **Specified account.** If you select this option, specify the account (username and password) that has the appropriate access rights. For example, for on-demand scans, the account should have access rights to the scanned object; for update tasks, the account should be able to access the shared folder on the Administration Server or to be authorized on the proxy server.

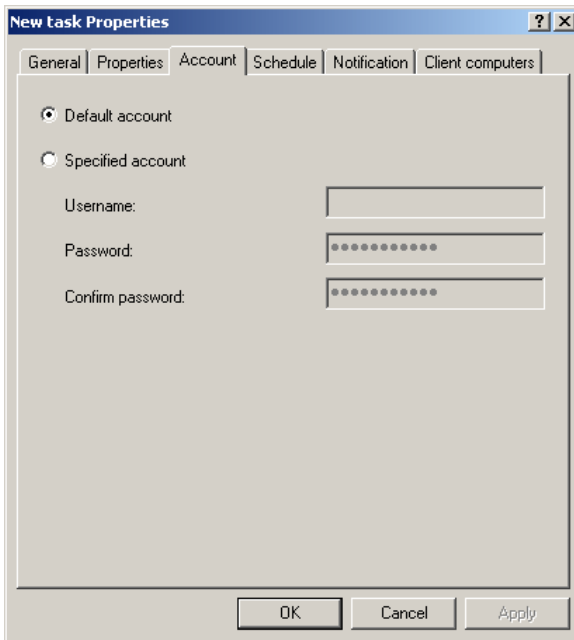


Figure 90. Editing task settings. The **Account** tab

This will avoid problems with on-demand scan and update tasks when the user does not have the required access rights.

On the **Schedule** tab (Figure 91) you can change task scheduling options. By pressing the Advanced button, you can:

- configure automatic startup of the operating system on the computers turned off at the time when the task is launched (details see section 3.2.6 on page 132);
- configure the computer to be turned off after the task is completed (see section 3.2.7 on page 132);
- restrict the duration of the task execution (details see section 3.2.8 on page 133).

The content of the **Schedule** tab and its operation are analogous to those available in the schedule settings configuration window that opens when you create a task (see section 3.2.1 on page 112).

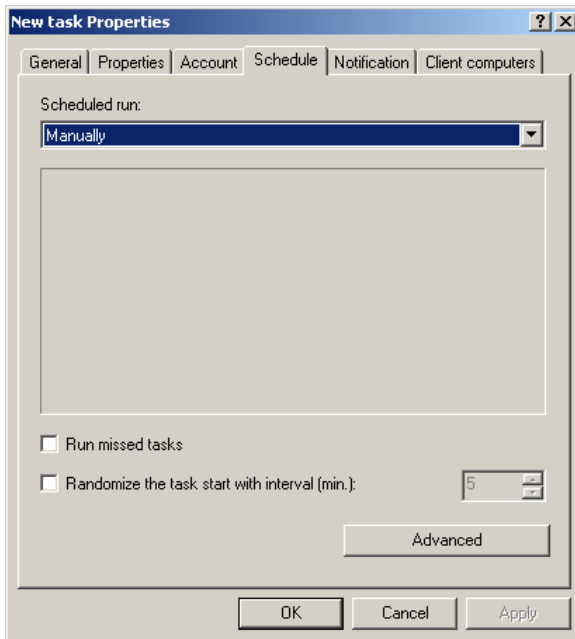


Figure 91. Editing task settings. The **Schedule** tab

On the **Notification** tab (Figure 92), you can configure settings for sending notifications about task performance results.

- In the **Register information about task history** fields, specify how for the task history is stored:
  - Check the **Store task history locally** to store information locally on each client.

This option is available for Kaspersky Anti-Virus 5.0 for Windows File Servers only.

- Check the **Store task history on the server for (days)** to store centrally task history, sent from all clients, on the Administration Server. In the field to the right, specify the interval for which the task history will be stored on the server. When the specified period has elapsed, the information will be deleted from the server.
  - **In Windows Event Log on Client** checkbox: to save event information in Windows event log local to each client.
  - **In Windows Event Log on Administration Server** checkbox: to save application execution data from all clients centrally in Administration Server Windows event log.

Use the same field to specify which events are to be logged:

- **Log All.**
  - **Log Task Progress.**
  - **Log Execution Result Only.**
- In the **Notify administrator** group, specify the type of task results about which you (and other users) want to receive notifications, and configure notification settings.

Set one or more checkboxes:

- **Email Notification:** send notifications through a mail server.
- **Use NET SEND:** send network notifications using the NET SEND service.
- **Run Executable:** run a program or an executable when the event is raised.

Configuration is identical to that in the event properties under the **Notification** tab. Administration Server settings are used by default.

Check **Notify of all results** to receive notifications on all task performance events.

Check **Notify of every failure** to be notified about errors only.

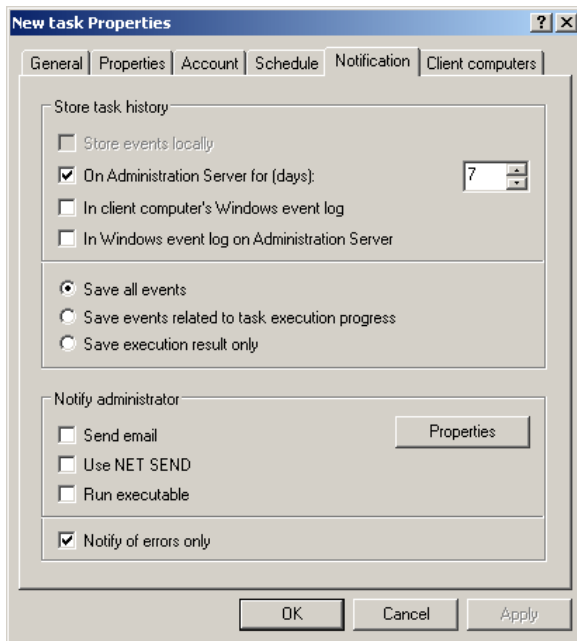


Figure 92. Editing task settings.  
The **Notification** tab

The global task properties dialog box has the **Target computers** tab (see Figure 93), which has a list of logical network clients on which the selected task is running. You can add and remove clients from the list.

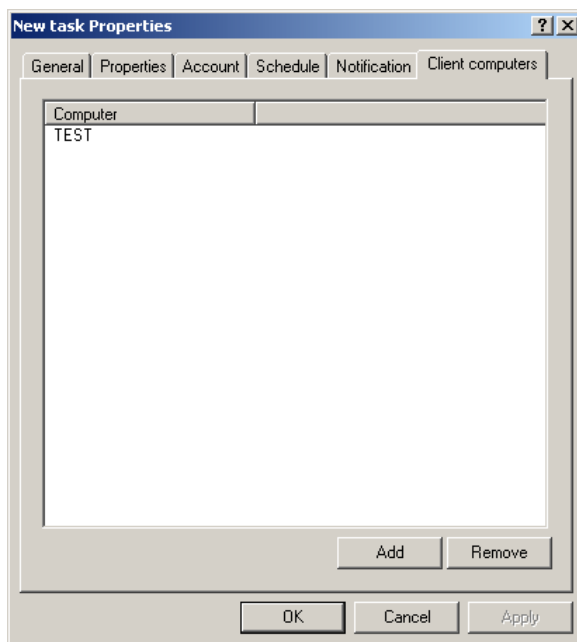



Figure 93. Editing global task settings.  
The **Client computers** tab

### 3.2.5. Displaying Inherited Group Task in Nested Group Result Pane

*To display inherited policies in a nested group under the **Group Tasks** folder:*

1. Select the **Group Task** folder in a nested group result pane.
2. Open a popup menu, select **Type** and check **Inherited Tasks**.

This will cause inherited group tasks to be displayed in the result pane marked with  Inherited group task properties may be viewed. Inherited group tasks may only be edited in a group under which they were created.

### 3.2.6. Automatic operating system loading on the client computers before the task execution

*To ensure that the task is executed on computers that are turned off at the time specified in the schedule,*

in the **Schedule** tab of the task configuring window (see Figure 91), press the **Advanced** button. In the window that will open, check the **Activate computer before the task is launched by function Wake On LAN (min)** box, and indicate the required time. As the result, the operating system of the computer will startup before the task is launched.

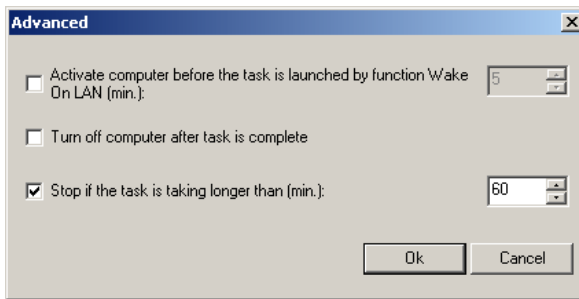


Figure 94. The **Advanced** window

### 3.2.7. Turning off the computer after the task completion

*To turn off the computer after the task is completed,*

on the **Schedule** tab in the task settings window (see Figure 91), press the **Advanced** button. In the window that will open (see Figure 94) check the **Turn-off computer after the task is completed** box.

### 3.2.8. Restricting time for the task execution

*To restrict task execution time,*

in the **Schedule** tab of the task configuring window (see Figure 91) press the **Advanced** button. In the window that opens (see Figure 94) check the **Stop if the task is taking longer then (min.)** and specify the time period in minutes after which the task will be stopped.

### 3.2.9. Canceling scheduled task launch

*To cancel the launch of a scheduled task,*

in the **General** tab of the task configuring window (see Figure 88) uncheck the **Schedule** box. As a result the task will remain in the list but will not be launched according to the schedule.

### 3.2.10. Creating application start / stop task

*To start/stop applications on client computers,*

create a group, global, or local task. In the task settings, you should specify the following:

- select **Network Agent** as the application, and **Start /stop application** as the task type.
- In the **Task settings** dialog box (see Figure 95), select one or more applications from the list by checking the boxes beside the applications' names. Select one of the following options in the drop-down box in the lower part of the window:
  - **Stop application**
  - **Start application**

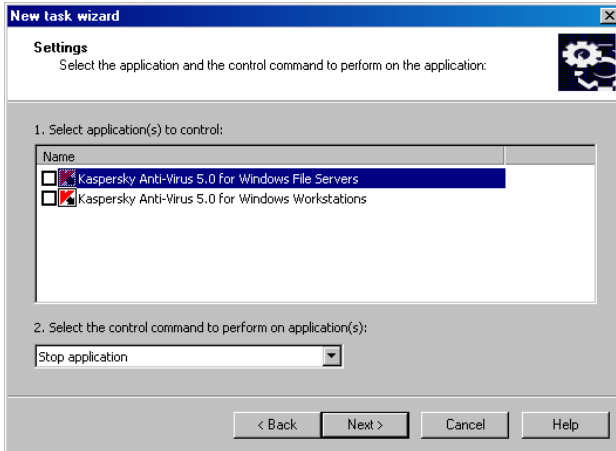


Figure 95. Start /stop application task.  
**Task settings** dialog box

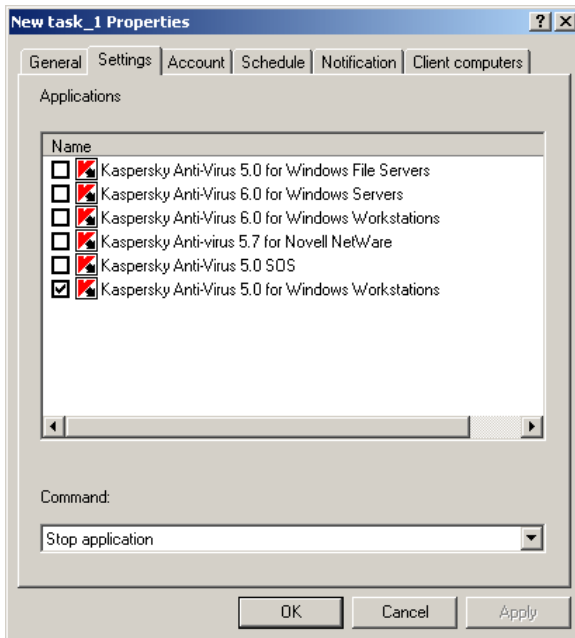


Figure 96. Editing the Start /stop application task

## 3.2.11. Exporting and importing tasks

*To export a task from the administration group to a file:*

In the console tree, select the required task and click the **Tasks** folder. The results pane will display a list of all tasks that exist for this group. Select a task, and click **Export** on the shortcut menu or on the **Action** menu.

In the window that opens, specify the name of the file where the task will be saved and its location. Click **Save**.

## 3.2.12. Importing a task

*To import a task from a file:*

In the console tree, select the required group. Open the shortcut menu of the **Tasks** folder and click **Import**. The same command can be accessed on the **Action** menu

In the window that opens, specify the name of the file from which the task will be imported and click **Open**.

## 3.2.13. Starting and stopping tasks manually

*To manually start/stop a task:*

In the details panel, choose the target task (either global or group) and open the shortcut menu. Click **Start / Stop** on the shortcut menu or on the **Action** menu.

## 3.2.14. Pausing/resuming tasks manually

*To pause/resume a running task:*

In the details panel, select the target task (either global or group) and open the shortcut menu. Click **Pause / Resume** on the shortcut menu or on the **Action** menu.

To perform the same operations, click the **Start**, **Stop**, **Pause**, or **Resume** buttons (see section 3.2.4 on page 124) on the **General** tab of the task properties dialog box.

Tasks are launched on a client only if the corresponding application is running. When the application is disabled, all running tasks are cancelled.

## 3.2.15. Monitoring task execution

*To start monitoring the task execution:*

open the settings window for the task you need (see section 3.2.4 on page 124) and switch to the **General** tab (see Figure ). The following information will be displayed in the lower part of the tab:

- **Pending** – number of computers for which the task settings have been modified on the Administration Server but the changes have not yet been synchronized with the client computer.
- **Scheduled** – number of computers for which this task is scheduled and synchronized with the Administration Server.
- **Paused** – number of computers on which this task is paused.
- **Running** – number of computers on which this task is running.
- **Completed** – number of computers on which this task has successfully been completed.
- **Failed** – number of computers on which the task failed.

Similar information for specific tasks is displayed in the program main window when you are viewing group or global task properties.

## 3.2.16. Viewing results of the task execution stored on the Administration Server

*To view the results of the task execution stored on the Administration Server:*

Open the **<Task name> Properties** dialog box for the desired task (see section 3.2.4 on page 124), select the **General** tab (Figure 97), and click **Results**.

This will open the **Task execution results** dialog box (see Figure 97). The top part of the dialog box contains the list of client computers for which this task is defined. The following information will be displayed:

- **Host** — name of the client computer on which the task is defined.
- **Group** — the name of the administration group that contains the client computer.
- **Status**— the current task status.
- **Time** — date and time of the last event registration.
- **Description** — detailed description of the task.

The bottom part of the box displays the results of the task execution on the selected client computer.

- **Status** — all changes in the task status.
- **Time** — date and time of the registration of each event.
- **Description** — detailed description of each event.

Information contained in the window includes data from the slave Administration Servers.

You can refresh information in each table by pressing the **Refresh** button.

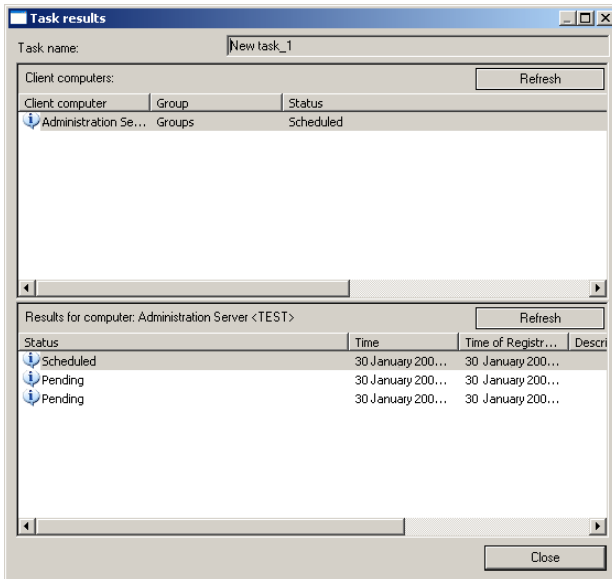


Figure 97. Viewing task history stored on the Administration Server

To view task performance results for each client, open the **<Computer name> Properties** dialog box using the **History** button on the **Tasks** tab (see below). You will see information stored on the Administration Server.

To view task performance results for each client, open the **<Computer name> Properties** dialog box using the **History** button on the **Tasks** tab (see below). You will see information stored on the Administration Server. If task history is stored locally on a workstation, use the administration console installed on this computer.

### 3.2.17. Configuring the event filter for a group task

To configure a filter for information displayed in the **Task results** window:

1. Use the **Filter** command of the shortcut menu in the list of the client computers. This will open a filter settings configuration window (see Figure 98). Configure the filter settings.

2. Select the event characteristics and task execution results that must be displayed after the filter has been applied, using the **Events** tab (see Figure 98).
  - Select the event importance level from the drop-down list.
  - To ensure that task execution results are displayed, select the required task status in the **Task execution results** field.
  - To restrict the amount of information to be displayed after the filter has been applied, check the **Restrict the number of displayed events** box and indicate the maximum number of rows to be included in the table.

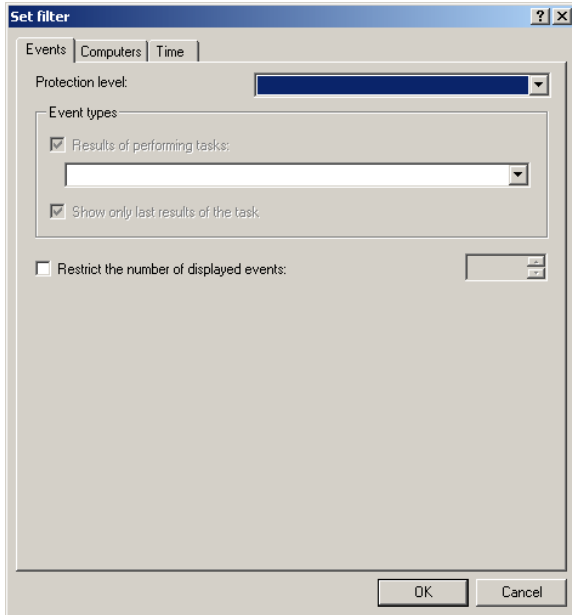


Figure 98. Configuring an event filter.  
The **Events** tab.

3. On the **Computers** tab (see Figure 99) determine computers on which the events and task execution results must be registered.  
You can use the following parameters:
  - **Computer name** in the logical network;
  - **Computer's name in the Windows network;**

- **Administration group;**
- **Domain;**
- **Range of IP-addresses** of the computers, by checking the corresponding box, and enter the start and end IP address for the range.

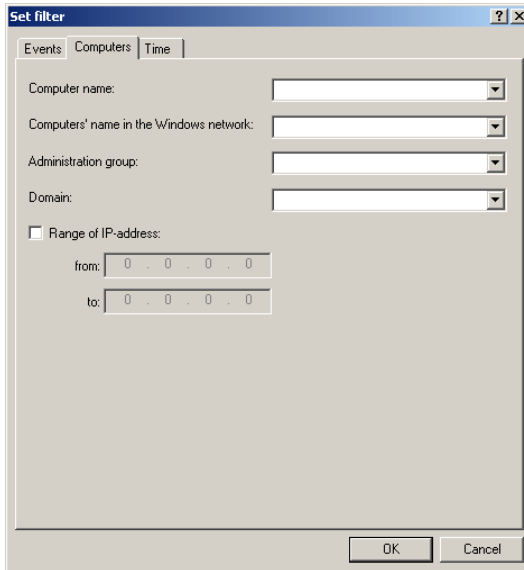


Figure 99. Configuring an event filter.  
The **Computers** tab

4. Define the event and task execution registration time on the **Time** tab (see Figure 102).

You can select the following options:

- **During a period**, and define fixed dates for the beginning and end of the period. Select **Events for date** in the **from** and **until** group of fields respectively, and specify dates and times. If all recorded information is required, select **First event** and **Last event**.
- **For the last days** and specify the number of days.

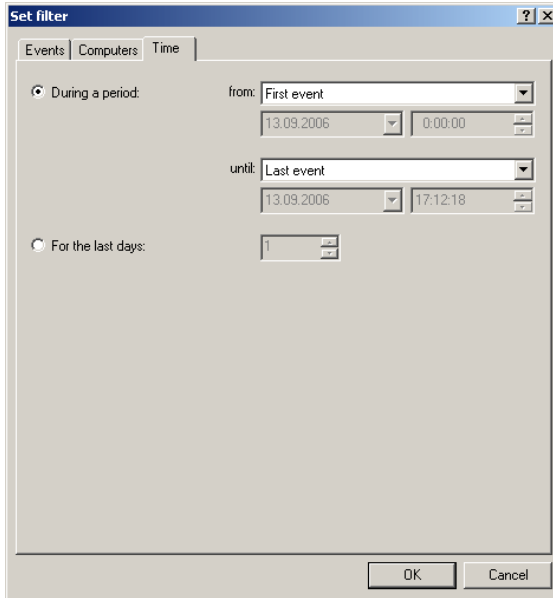


Figure 100. Configuring an event filter.  
The **Time** tab

5. After you have finished configuring settings for the filter, press the **OK** button. As the result, only data that comply with the specified settings will be displayed in the **Task execution results** window.

### 3.2.18. Configuring event filter for a selected computer

*To configure filter for the information displayed in the **Task execution results** window*

1. Select **Filter** from the shortcut menu. This will open a filter configuration window.
2. Configure filter settings on the **Events** (see Figure 101) and the **Time** tabs.

Select the event characteristics and task execution results that must be displayed after the filter has been applied, using the **Events** tab (see Figure 101).

- Select the event importance level from the drop-down list in the **Protection level** field.

For each application, there are defined events that may occur during its operation. Each event has a characteristic that reflects its importance level. Events of the same type may be of different importance level depending on the situation in which the events occurred.

- To configure the filter to include only events of a specific type, check the **Events** box and check boxes next to the names of the required types. If the event type is not specified all types of events will be displayed.
- To ensure that the task execution results are displayed, check the **Results of performing tasks** box and select the task status you are interested in.
- To obtain information only about results of the last task launch, check the **Show only last results of the task** box.
- To restrict the amount of information to be displayed after the filter has been applied, check the **Restrict the number of displayed events** box and indicate the maximum number of rows to be included in the table.

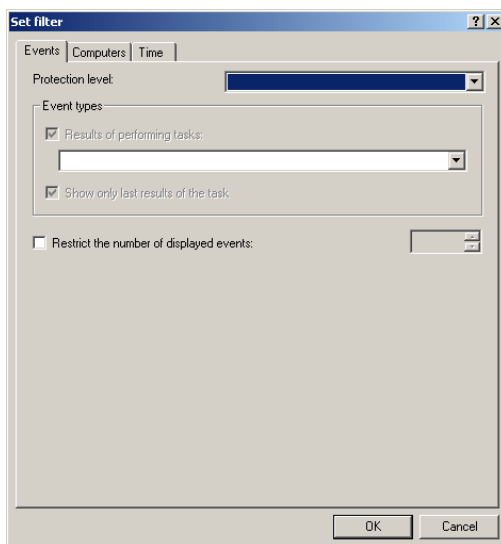


Figure 101. Configuring an event filter.  
The **Events** tab.

Using the **Time** tab configure settings similarly to the settings for a group task (see section 3.2.17 on page 138). The **Computer** tab is not provided as the filter is configured for a selected computer only.

3. To confirm the changes, press the **OK** button. The filter means that only information that satisfy the specified parameters will be displayed in the **Task execution results** window.

### 3.2.19. Removing a filter

*To remove the filter,*

Use **Remove filter** command from the shortcut menu.

---

# CHAPTER 4. UPDATING THE ANTI-VIRUS DATABASE AND PROGRAM MODULES

## 4.1. Downloading updates by the Administration Server

### 4.1.1. Creating task for receiving updates by the Administration Server

Downloading updates by the Administration Server is a global task (see section 3.2.2 on page 122). To create the downloading updates task, select **Kaspersky Administration Kit** as the application for which you want to create the task, and the **Download updates task** as the task.

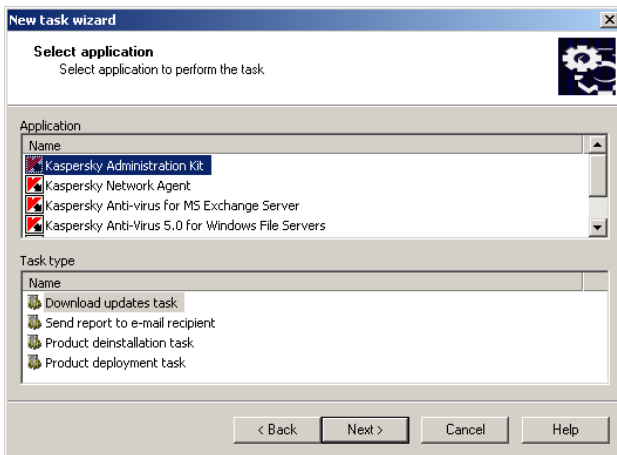


Figure 102. Creating an update task.  
Selecting the application and the type of task.

When configuring the task (see Figure 103) create the list of update sources. You can configure settings for connection with the updating servers, and

determine whether slave Administration Servers will automatically launched their update tasks after the master Server has received updates.

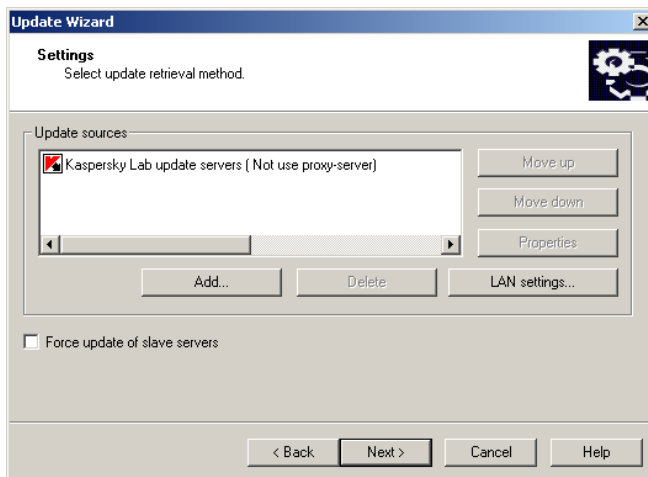


Figure 103. Creating an update task.  
Configuring updates receiving settings

You can create the list of updates sources using the **Add...** and the **Delete** buttons.

To add an updates source to the list, press the **Add...** button and select one of the following options in the **Updates source properties** window that will open (see Figure 104):

- **Kaspersky Lab's update servers** - for receiving updates via Internet, using Kaspersky FTP and HTTP servers. You can modify the proxy server settings in the task configuration window.
- **Master Administration Server** - for receiving updates from the public folder of the Administration Server.
- **Update folder** - for receiving updates from a network folder. If you select this option, specify the address of the folder that contains the updates.

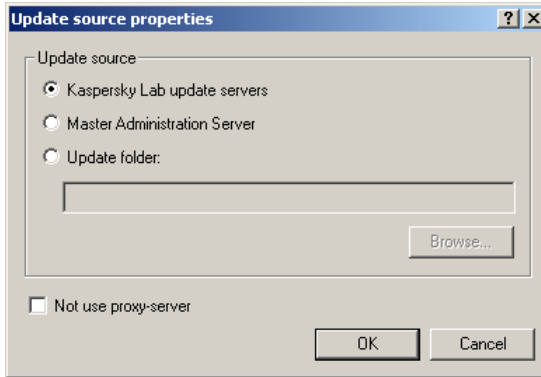


Figure 104. Configuring the updates source

Check the **Not use proxy-server**, if you don't want to use proxy when connecting to updates source. If the box is checked, The proxy-server will be used according to the settings specified in **LAN settings** window.

Kaspersky Anti-Virus will perform the update from the sources in the list in the order they are listed. If this source is unavailable for any reason, the updating will be performed from the source next in the list, and so on. You can change the order of the sources in the list using the **Move up** and **Move down** buttons.

To configure connection to the updates server, press the **LAN settings...** button and specify the required values of the parameters in the window that opens (see Figure 105).

- If you connect to the updates server via a proxy server, check the **Use proxy server** box and enter the address and the port number to be used to connect to the proxy server. Only decimal notation is allowed (for example, **Address** 125.2.19.1, **Port**: 3128).
- If a password is used to access the proxy server, define the proxy user authentication parameters. To do this, check the **Proxy server authentication** box and fill the **Username** and **Password** fields.
- Check the **Use passive FTP mode** to use passive mode when the update is performed using the FTP protocol, or uncheck the box to use the active mode. You are advised to use passive mode.
- Using the **Connection timeout, sec** field, specify the maximum time for connecting to the updates server. If the connection has failed, after the specified period of time an attempt will be performed to connect to the next updates server`.

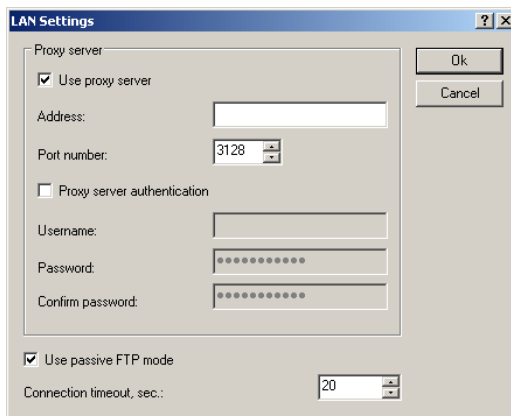


Figure 105. Configuring the parameters used to connect to the updates server

To ensure that tasks to download updates onto slave Administration Servers are launched automatically after the master server receives the updates, irrespective of the schedule configured in the settings of these tasks, check the **Force update of slave servers** box.

Check **Advanced Troubleshooting** to log task detail. If the checkbox is unchecked, only major task execution phases will be logged.

## 4.1.2. Configuring the update task

On the **Settings** tab, you can change update task settings as follows:

- Define the contents of the updates to be downloaded from an update source in the **Update sources** group of fields (see section 4.1.1 on page 144). To do this, select one of the following options:
- Define update components to be downloaded from a source by clicking the **Update Components** button and using the checkboxes in the resulting dialog (see Figure 116) to include the required update components:
  - **Download all available updates**
  - **Download updates for all Kaspersky Lab applications installed on network**
  - if updates to the anti-virus database and application modules are to be downloaded, check the boxes beside the types of updates desired, in the table in the bottom section of this window.

Antivirus database updates and program patches are saved in the specified shared folder on the Administration Server.

- manage the automatic launch of the task for receiving updates by slave Administration Servers using the **Force update of slave servers** box;
- view the location of the folder containing the updates received from the source in the **Local updates source folder** field.
- control the level of detail in the task log using the **Advanced Troubleshooting** checkbox.

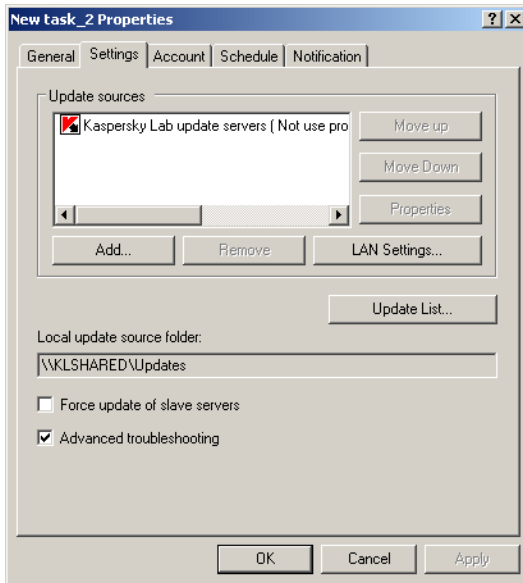


Figure 106. Configuring the update task.  
The **Settings** Tab

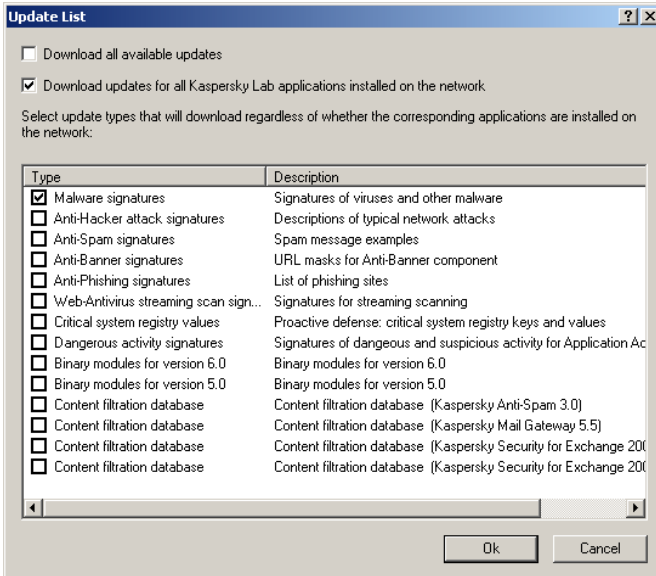


Figure 107. Selecting the update

### 4.1.3. Viewing the list of updates

*To view the updates received by the Administration Server,*

select the **Update** node in the console tree. The list of the updates downloaded by Administration Server will be displayed in the results pane.

### 4.1.4. Viewing properties of the downloaded updates

*To view update properties:*

Select the required update in the details panel and click **Properties** on the shortcut menu or on the **Action** menu. This will open the **<Update name> Properties** dialog box (see Figure 108).

The **General** tab displays the following information:

- Update name; for the anti-virus database updating the field contains value **Anti-virus signatures**.

- Number of records in the anti-virus database (this field is missing for application modules updates);
- Name and version of the application to which the update applies;
- Size of the update saved on the Administration Server
- Date when the update was copied to the Administration Server
- Date of anti-virus database creation.

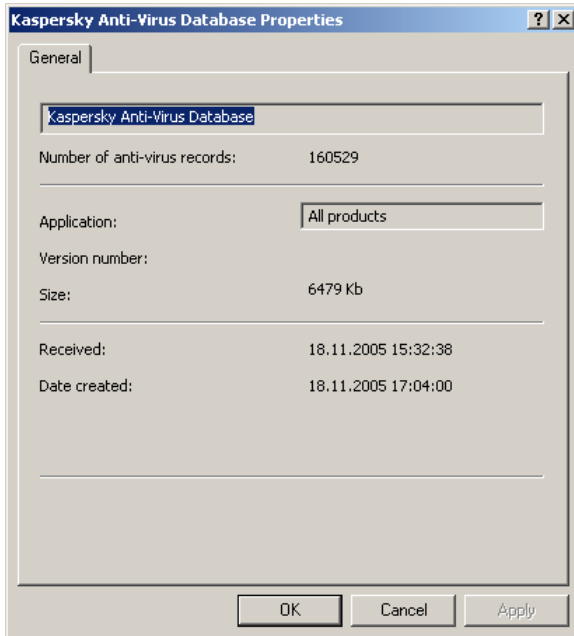


Figure 108. Viewing properties of the downloaded update

## 4.2. Automatic distribution of updates

### 4.2.1. Automatic distribution of updates on the client computers

*To make the server push updates to clients immediately after downloading:*

In Kaspersky Lab application's update task settings set Administration Server as an Update source, and select **On receipt of updates by the Administration Server** in **Settings** tab.

### 4.2.2. Automatic distribution of update to the slave servers

*To ensure that updates received by the master Administration Server are automatically distributed to slave servers immediately after they are received,*

in the settings of the Administration Server's receiving updates task, check the **Force updating of slave servers** box.

As the result, immediately after the updates are received by the master Administration Server, tasks of receiving updates by the slave Administration Servers will be automatically launched irrespective of the scheduled specified in the settings of these tasks.

### 4.2.3. Creating the list of the updating agents and configuring the agents

*To create a list of updating agents and configure them to distribute updates on the computers within a group,*

switch to the **Update Agent** tab (see Figure 109) in the group properties window (see Figure 24). Using the Add and Remove buttons, create the list of computers that will be used as the updating agents within the group.

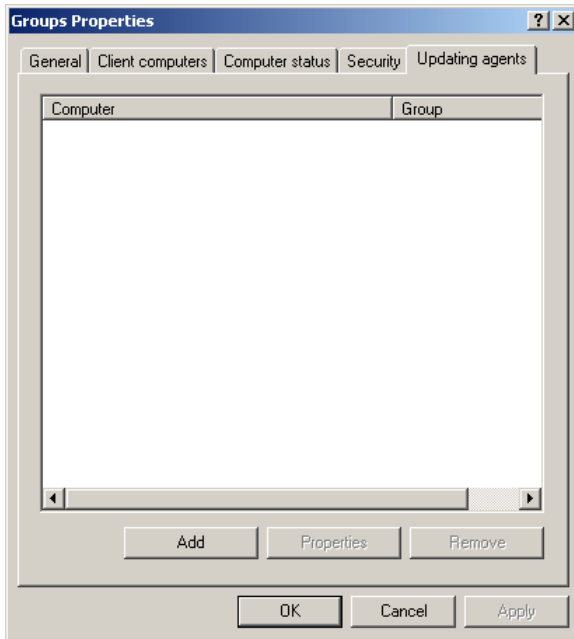


Figure 109. The group properties window  
The **Update agents** tab

To configure an updating agent, select the agent in the list and press the **Properties** button. In the **<Updating agent's name> properties** window you can:

- specify the number of the port via which the client computer will be connected to the updating agent. The default value is **14000**;

If the host running the Administration Server is specified as the Update Agent, port **14001** is used by default .

- specify the number of the port via which the client computer will be securely connected to the updating agent using SSL protocol. By default port **13000** will be used.

If the host running the Administration Server is specified as the Update Agent, port **13001** is used by default for an SSL connection.

- enable the use of multi-address IP delivery for automatic distribution of installation packages to client computers within the

group,. by checking the box **Use multicast** and fill the fields **Multicast IP** and **Port Number**.

- **IP-MULTICAST Port number** For details on the distribution of installation packages using updating agents, see the Implementation guide.

To view update agent statistics, click the **View Update Agent Statistics** link.

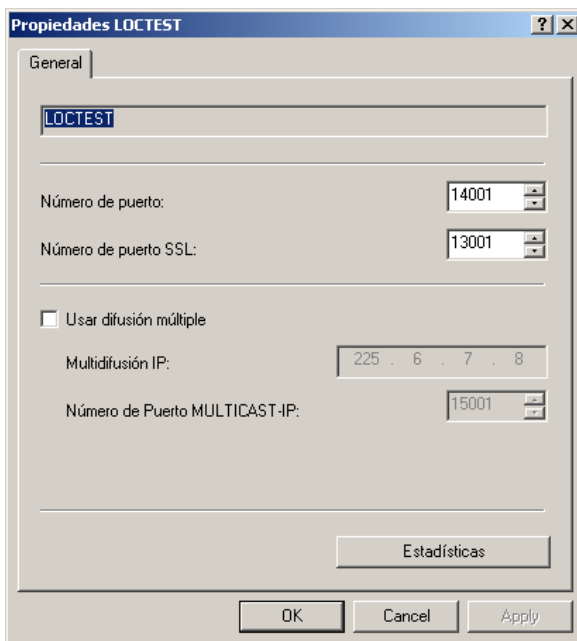


Figure 110. The Updating agent properties window

---

# CHAPTER 5. MAINTENANCE

## 5.1. Renewing your license

### 5.1.1. Viewing information about installed license keys

*To view information about installed license keys:*

connect to the corresponding Administration Server (see section 2.1 on page 11) and select the **License keys** node in the console tree. The result panel will display the list of license keys installed on the client computers.

The following information will be displayed for each key:

- **Number** – license key serial number.
- **Key type** - the type of the license key installed, for example: **commercial, trial**.
- **Restrictions** – license restrictions imposed by the key.
- **License period** – the validity period of the license key.

### 5.1.2. Viewing license key details

*To view information about a specific license key:*

select the required license key in the results panel, and use the **Properties** command in the shortcut menu or in the **Action** menu.

This will open a **Properties: <key serial number>** dialog box which includes the **General** and **Objects** tabs (see Figure 113).

The following information is displayed in the **General** tab (see Figure 61):

- license key serial number;
- key type;
- license period;
- license restrictions imposed by the key.

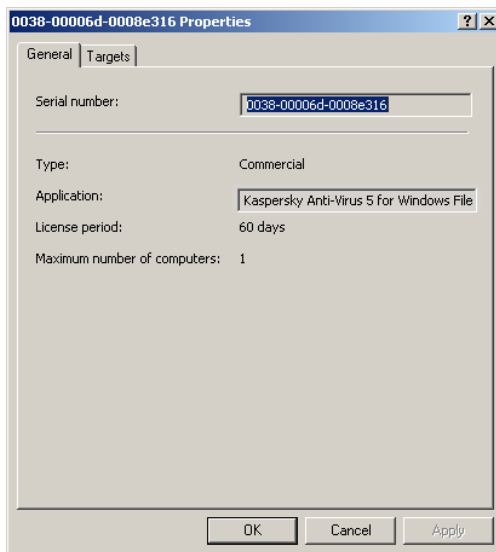


Figure 111. License key properties.  
The **General** tab

The **Targets** tab contains the list of client computers on which this license key is installed. The tab contains the following information:

- name of the client computers;
- administration group;
- whether or not this key is used as the current key;
- license expiration date;
- date of activation of the key on the client computer.

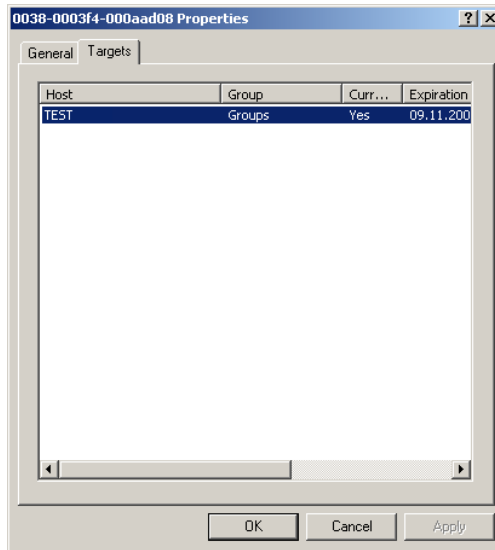


Figure 112. License key properties.  
The **Targets** tab

You can check which license keys are installed for the application on a specific client computer, by viewing the application properties configuration window.

### 5.1.3. Installing a license key

*To install a license key,*

create and launch a **license key installation** task.

The license key installation task can be created as a group, global or local task (see section 3.2.1). When creating this task:

- Specify the application for which you are installing this license key as the application for which the task is being created;
- specify **License key installation** as the task type.

During the task configuration state (see Figure 115), specify the license key file (\*.key) that must be installed.

If this key is intended to be used as the current key for the application and to immediately replace the previous current key, check the **Use as the current license key** box. If you are adding the key as a backup key, do not check this box. The backup license key becomes the current license

key upon the expiry of the current key. The **License key info** field contains detailed information about the license key.

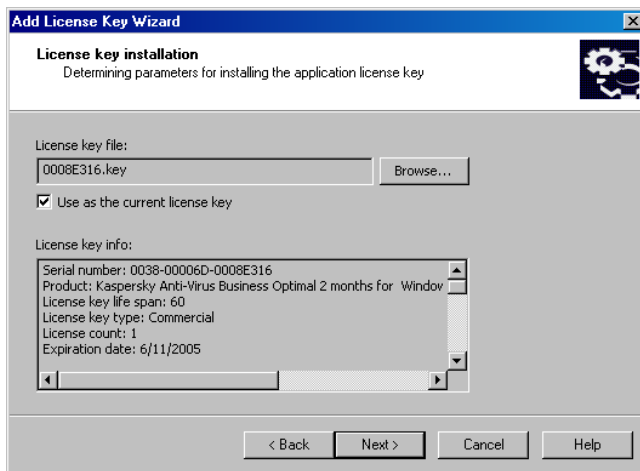


Figure 113. Creating a License renewal task.  
Selecting the license key file

## 5.1.4. Running the License key installation task creation wizard

To launch the **License key installation** task creation wizard:

Select the **License key** node in the console tree, and use the **Add license key** command in the shortcut menu or the analogous item under the **Action** menu. This will launch a global task creation wizard; this wizard will miss the step which selects the task type, as the task type will be selected by default.

Tasks created using the license key installation task wizard are global tasks and are located in the **Global task** node of the console tree.

When configuring the license key installation task on the **Settings** tab (see Figure 112), you can replace the license key file and check the box **Use as the current license key** to use the new key as the application's current key. If this box is unchecked, the key will be used as the backup key. The **License key info** field contains detailed information about the license key.

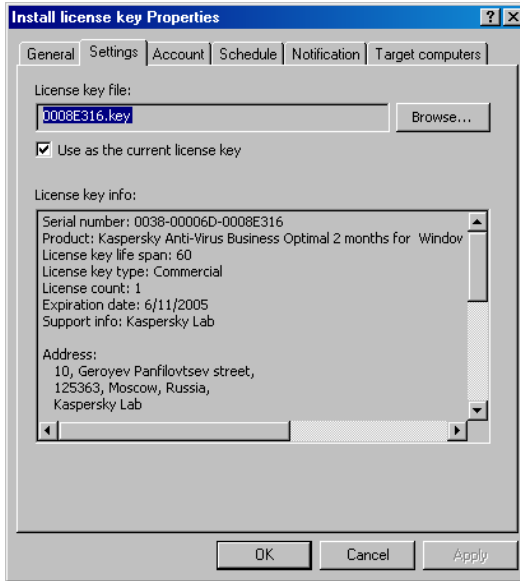


Figure 114. Configuring License renewal task.

### 5.1.5. Creating and viewing license keys report

*To generate a report about the status of the license keys installed on the client computers within the logical network:*

use a built-in template **License key report** or create a new template of the same type (see section 5.4.1 on page 167).

The report is created based upon the **License key report** template, and contains complete information about all license keys (both current and backup keys) installed on all client computers within the logical network, indicating which computers are using which keys, and the license restrictions.

## 5.2. Quarantine and backup storage

### 5.2.1. Viewing properties of quarantined or backed-up objects

*To view the properties of a quarantined or backed-up object:*

in the console tree, select the **Storages** node, then the **Quarantine** (or **Backup storage**) node. Select the required object in the results pane, and click the **Properties** command from the shortcut menu or the analogous item in the **Action** menu.

The window that opens will contain the following information about the object:

- name under which the object was delivered for processing by the anti-virus application;
- object description;
- action that was performed on the object by the anti-virus application;
- name of the computer on which the object is stored;
- status assigned to the object by the anti-virus application;
- name of the virus contained or possibly contained in the object;
- date when the object was quarantined or placed in backup storage;
- object size (in bytes);
- path on the client computer to the folder in which the object was originally located;
- name of the user who quarantined the object or placed it into the backup storage;

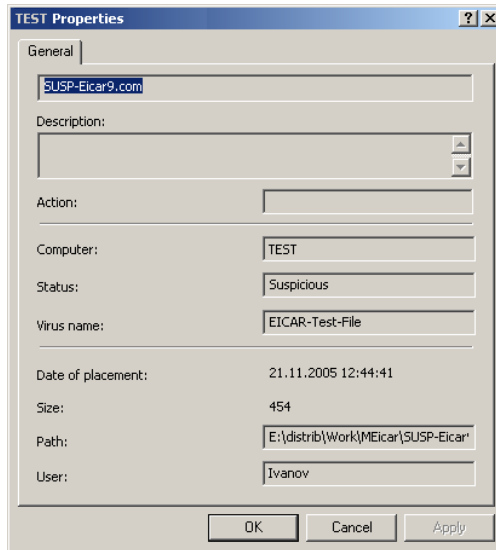


Figure 115. Viewing properties of a quarantined object

## 5.2.2. Removing objects from the quarantine or backup storage

*To remove an object from the quarantine or backup storage:*

in the console tree, select the **Storages** node, then the **Quarantine** (or **Backup storage**) node. Select the required object in the results pane and use the **Delete** command from the shortcut menu or the analogous item in the **Action** menu.

The anti-virus application that quarantined this object or placed it into backup storage on the client computer will remove the object from the quarantine or from the backup storage.

## 5.2.3. Restoring objects from the quarantine or backup storage

*To restore an object from a storage area:*

in the console tree, select the **Storages** node, then the **Quarantine** (or **Backup storage**) node. Select the required object in the results pane,

and use the **Restore** command from the shortcut menu or the analogous item in the **Action** menu.

The anti-virus application that quarantined this object or placed it into the backup storage on the client computer, will restore the object from the quarantine or from the backup storage.

## 5.2.4. Scanning the quarantine folder on the client computer

To scan the quarantine folder on the client computer:

in the console tree, select the **Quarantine** node. Select the object you wish to scan in the results panel and use the **Scan quarantined objects** command from the shortcut menu or the analogous item in the **Action** menu.

As the result, the on-demand quarantine folder scan task will be launched on the client computer for the anti-virus application that quarantined the selected object.

## 5.3. Event logs. Event queries

### 5.3.1. Viewing Kaspersky Administration Kit event log stored on the Administration Server

To view the Kaspersky Administration Kit event log stored on the Administration Server:

connect to the Administration Server (see section 2.1 on page 11), open the **Events** node in the console tree and select the required folder from the following: **All Events**, **Information messages**, **Critical messages**, **Functional failure**, **Warnings**, **Audited Events**.

In the details panel, you will see a table (see Figure 116) listing all events stored on this Administration Server, for all groups and installed applications, of the selected level of importance. The table has the following columns:

- **Severity** – level of event importance
- **Host** – client or Administration Server name associated with the event

- **Group** – name of the group that includes this client
- **Application** – application that generated the event
- **Version** – application version
- **Task** - name of the task that caused the event to occur.
- **Event** – event name
- **Time** – time when the event was logged
- **Description** – event description.

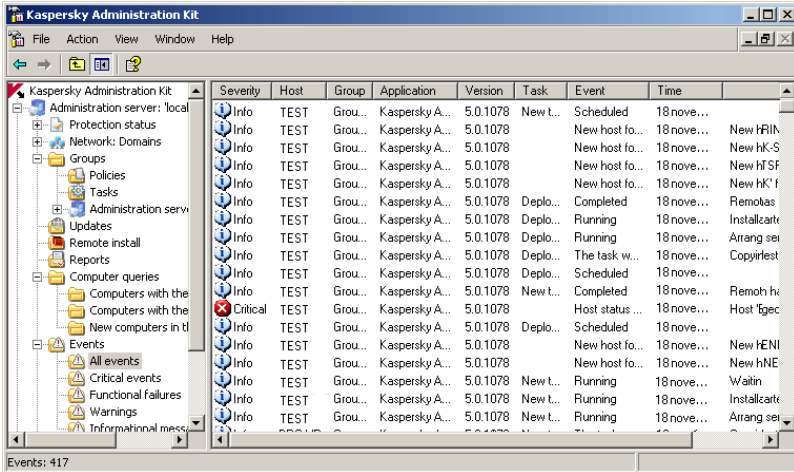


Figure 116. Viewing events stored on the Administration Server

You can sort data in any column in either ascending or descending order, change the order of columns, or add and remove columns.

To facilitate viewing and searching for required information, there is a provision for creating and configuring user-defined queries. The use of queries allows searching for and filtering out unnecessary information. This is very important since the Server stores a considerable amount of information.

### 5.3.2. Creating event queries

*To create a query:*

1. In the console tree, select the Events node., Open the shortcut menu and use the **New / New events query** command or the analogous item in the **Action** menu.

2. In the window that opens, enter the name of the query (see Figure 117) and press the **OK** button.

A new folder will be created in the console tree with the name that you specified for the query; the structure of this folder will include all events and task execution results that are stored on the Administration Server. To filter the events you must configure the query parameters.

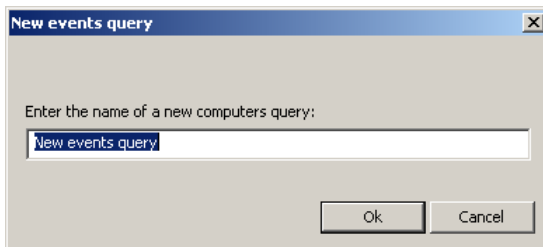


Figure 117. Creating an events query

### 5.3.3. Customizing event queries

*To customize a query:*

1. Select the required event query in the console tree or in the results panel, and use the **Properties** command from the shortcut menu or the analogous item in the **Action** menu.
2. This will open the query configuration window that contains the tabs: **General**, **Events**, **Computers** and **Time**.

On the **General** tab you can change the query name.

Using the **Events** tab define the event characteristics and task execution results that must be included in the query:

- Name of the application for which you require information.
- Application version number.
- Name of the task the results of which must be displayed.
- Select the level of the event importance from the drop-down list.

There are types of events defined for each application that occur during the application's operation. Each event has a defined level of importance. Events of the same type can be of different levels of importance depending on the situation in which the event occurred.

- To configure the query to include only events of a specific type, check the **Events** box and check boxes next to the names of the required types. If the event type is not specified all types of events will be displayed.
- To ensure that the query includes task execution results, check the **Results of performing tasks** box and select the task status you are interested in.
- To obtain information only about results of the last task launch, check the **Show only last results of the task** box.
- To restrict the amount of information to be displayed in the query, check the **Restrict the number of displayed events** box and indicate the maximum number of rows to be included in the table.

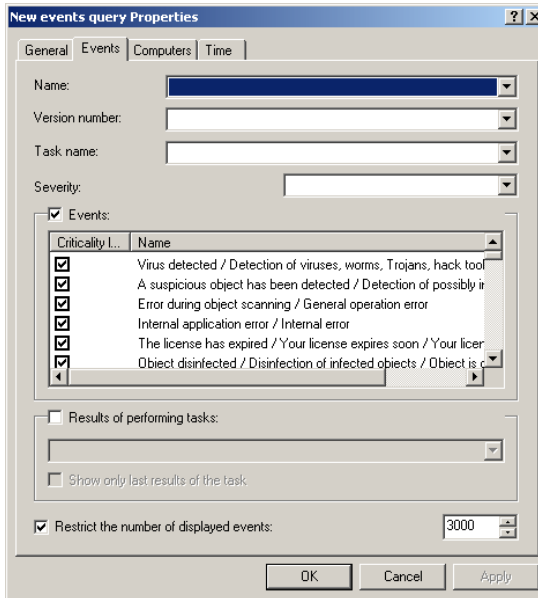


Figure 118. Configuring an events query.  
The **Events** tab

Using the **Computers** tab define on which computers events and task execution results included in the query must be registered. You can use the following parameters:

- Computer name in the logical network;
- Computer's in the Windows network;

- administration group;
- domain;
- specify the range of IP addresses of computers by checking the **Range of IP addresses** box and enter the start and end IP address.

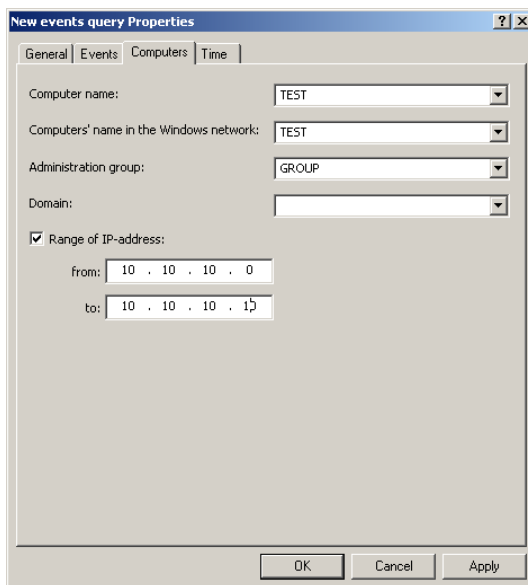


Figure 119. Configuring events query.  
The **Computers** tab

Specify time for registration of events and task execution results on the **Time** tab (see Figure 131).

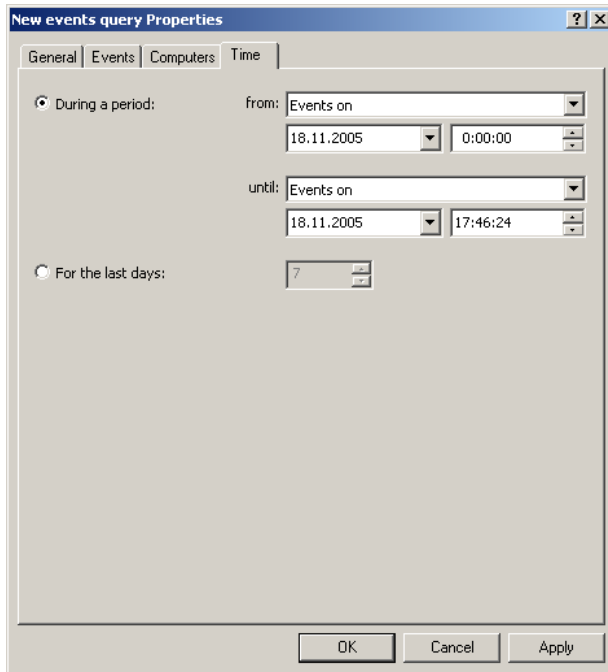


Figure 120. Configuring events query.  
The **Time** tab

You can select the following options:

- **During a period** and specify dates for the beginning and the end of the period. To do this, select **Events for the date** in the field groups **from** and **until** and specify the exact date and time. If all registered information is required, select the **First Event** and the **Last event**.
  - **For the last days** and specify the number of days.
3. To confirm your changes, press the **Apply** or **OK** button. The Events table will display only information that satisfies the new criteria.

### 5.3.4. Saving information about events to a file

*To save events information to a file:*

1. Select in the console tree the event query that contains the events you need, and use the All tasks/Export command in the shortcut menu or the analogous item in the Action menu. This will launch the wizard.
2. During the first step of the wizard, specify the file's path and name in which the information will be saved. If you want only those events that you selected in the results panel to be saved to the file, check the **Export selected events only** box.
3. During the second step, select the file format:
  - **Export as a text , divided by tabulation marks** - text file
  - **Export as UNICODE text , divided by tabulation marks** - UNICODE format text file.
4. To close the wizard, press the **Finish** button.

### 5.3.5. Deleting events

*To delete events satisfying certain criteria:*

Create and apply an event query with the desired criteria. After this delete the events on the results panel using the **Delete** option on the shortcut menu.

The application will only delete the events that satisfy query settings from the **Events** node.

## 5.4. Reports

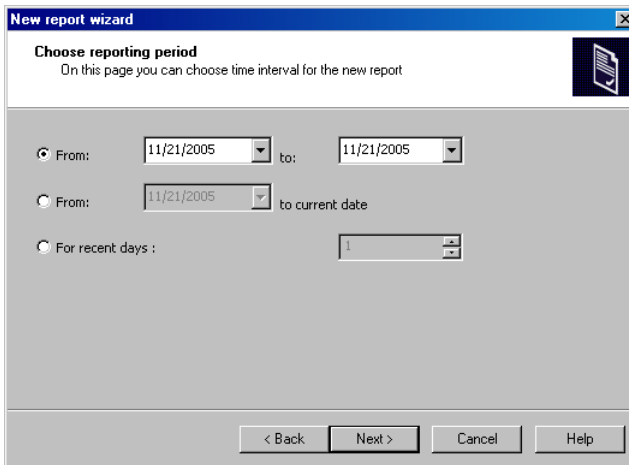
### 5.4.1. Creating a report template

*To create a report template:*

1. Choose the **Reports** node in the console tree and click the **New** command on the shortcut menu or on the **Action** menu to start a wizard. Follow the wizard's instructions.

2. Specify the template name. If a template with this name already exists, the **\_1** ending will be automatically added to the new template name.
3. Choose the report type. The following steps will depend on your choice.
4. Specify the reporting period. You can set fixed reporting dates or leave the end date open. In the second case, the program will use the current system date as the end date for the report. You can also select the **For recent days** option and specify the number of days in the field on the right.

This step is not required for reports reflecting the current state – for example, for reports on the current anti-virus protection.



The screenshot shows a window titled "New report wizard" with a sub-header "Choose reporting period". Below the sub-header is the instruction: "On this page you can choose time interval for the new report". There are three radio button options for selecting the reporting period:

- From: 11/21/2005 to: 11/21/2005
- From: 11/21/2005 to current date
- For recent days : 1

At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

Figure 121. Creating a report template. Defining the reporting period

5. Specify objects for which you want to create the report.
  - **I want to create a report for a group** – create a report for computers included in one group
  - **I want to create report for a list of computers** – create a report for computers from different groups

If a report can only be created for the entire network, for example **Licensing report**, this step and the next one are omitted.

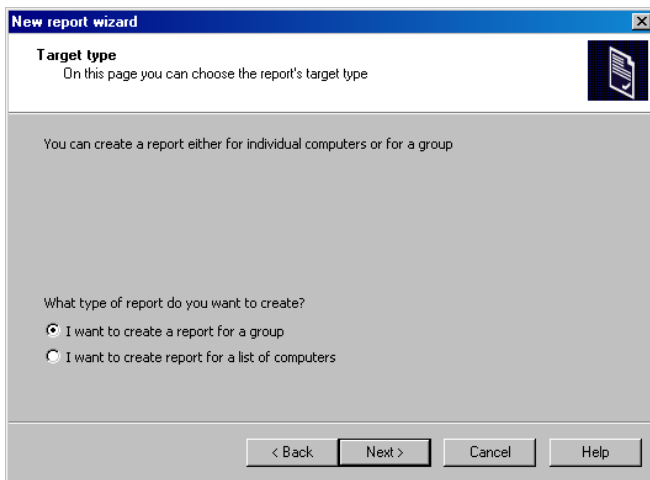


Figure 122. Creating a report template. Selecting objects to be reported.

6. Specify the group or select specific clients from different groups for which you want to create a report, and close the wizard.

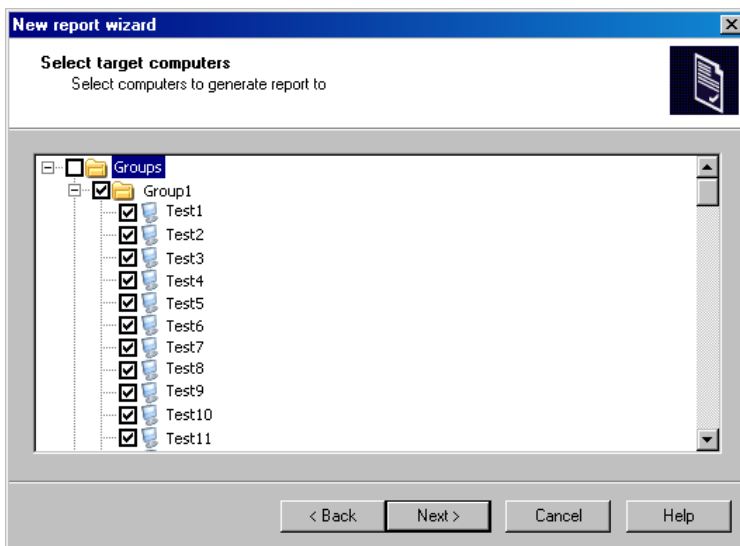


Figure 123. Creating a template for protection reports. Selecting clients

After you close the wizard, the new template will be added to the **Reports** node in the console tree and displayed in the details panel. The template can be used to create and view reports.

## 5.4.2. Viewing and editing report templates

*To view and/or modify a report template:*

Connect to the Administration Server (see section 2.1 on page 11) and select the **Reports** node in the console tree. A list of existing report templates will be displayed in the details panel. Choose the required template and click **Properties** on the shortcut menu or on the **Action** menu.

This will open the **<Report template name> Properties** dialog box (see Figure 124). The tabs in this dialog box are specific to each report type.

The **General** tab contains general information about the template. On this tab you can:

- change the name of the report template.
- view the name of the template type, its description, date and time of its creation and the latest change to the settings;
- add to the report information from the slave Administration Server (see section 5.4.4 on p.177).
- restrict the number of records included in the report (see section 5.4.5 on page 178);
- check the **Print version** box so that the report created will be displayed in a format suitable for printing;
- enable utilization of data from slave Administration Servers using the **Configure Settings for Administration Server Hierarchy**;
- create a report based on a template, by pressing the **Generate...** button.

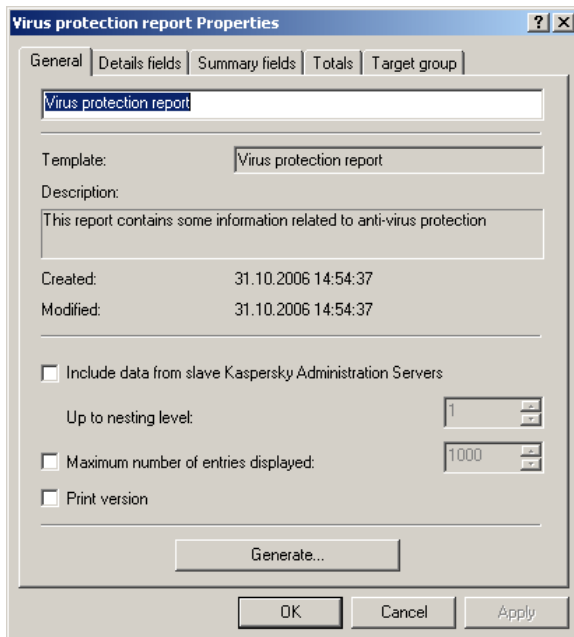


Figure 124. The report template settings window.  
The **General** tab

The **Period** tab is used to specify the time period for which the report is created. Its settings are similar to those provided in the **Reporting period** window (see Figure 121) in the report template creation wizard.

The **Details fields** tab (see Figure 125) is used to define the fields included in the report's detailed field table, together with the record sorting order, and filter settings. To create the list of fields use the **Add...** and **Delete** buttons. The field order may be changed with the **Move Up** and **Move Down** buttons. Sorting order in a field may be modified, and filtering specified, using the **Edit** button. Use the resulting window (see Figure 126) to set the following parameters:

- to set sort order for records in the selected field, check **Sort Report Fields** and select **Ascending** or **Descending**;
- to use records in the filter field, check **Filter Field Values** and specify criteria in the fields below. Each report field has its own set of filtering criteria.

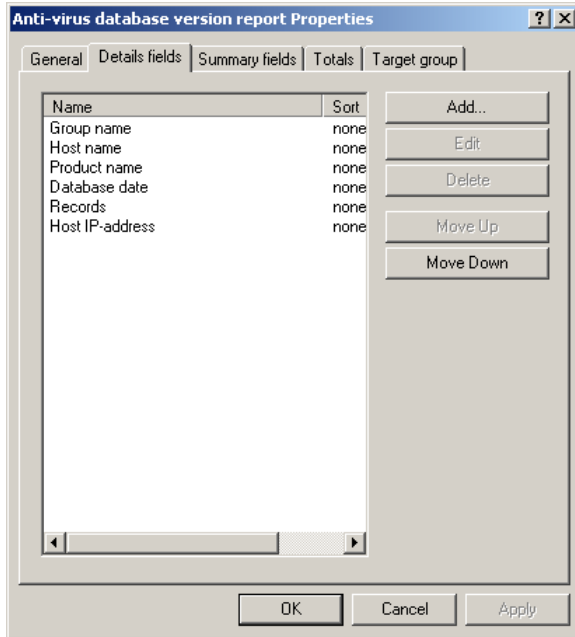
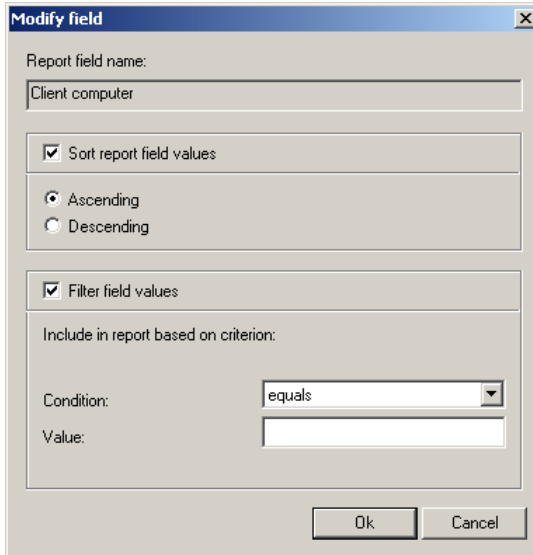


Figure 125. The report template settings window.  
The **Details fields** tab



The image shows a 'Modify field' dialog box with the following settings:

- Report field name: Client computer
- Sort report field values
  - Ascending
  - Descending
- Filter field values
- Include in report based on criterion:
  - Condition: equals
  - Value: (empty)

Buttons: Ok, Cancel

Figure 126. Selecting the order of the report fields sorting

On the **Summary fields** tab (see Figure 127), fields that form a table with summary data included in the report are defined as well as the sort order of the records pertinent to these fields. Settings of this tab (except for filtering) are similar to those provided on the **Details fields** tab (see Figure 125).

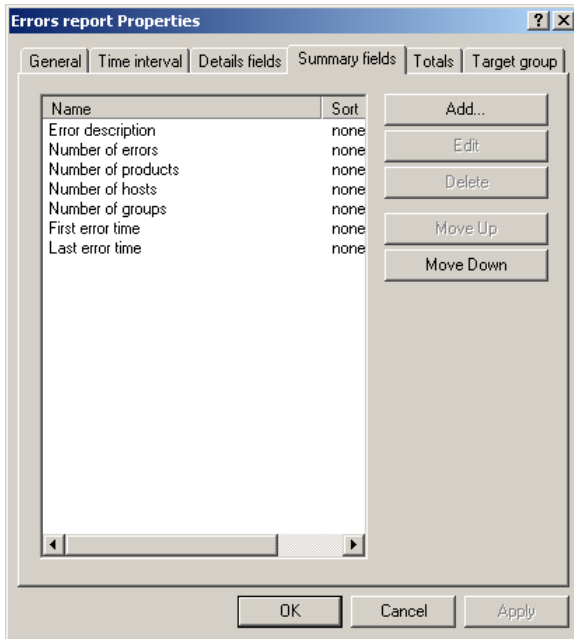


Figure 127. The report template settings window.  
The **Summary fields** tab

The **Totals** tab (see Figure 128) contains calculated fields of the report. To delete an object from the report template, select it in the **Details fields** list and press the **Remove** button. To add a field to the report template, select it in the **All fields** list and press the **Add>>** button.

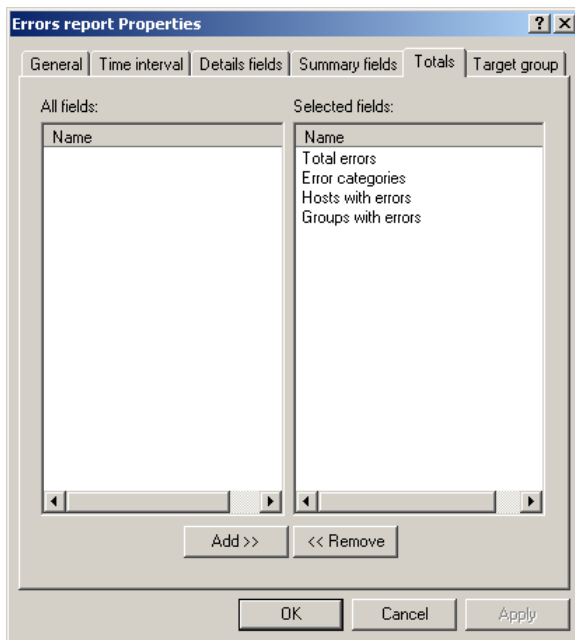


Figure 128. The report template settings window.  
The **Calculated fields** tab

The **Target group** tab indicates the group or a set of client computers for which information is included into the report. Its settings are similar to those provided in the corresponding window (see Figure 123) in the report template creation wizard.

Click the **Apply** or **OK** button to apply the settings.

### 5.4.3. Generating and viewing reports

*To generate a report using a template:*

in the console tree, connect to the target Administration Server and select the **Reports** node. In the details panel, you will see a list of available report templates. Select the required template and click the **Generate** command on the shortcut menu or on the **Action** menu to generate a report.

To view the report, a browser window with the generated report will open. The report contents correspond to the selected template and can have the following items:

- Company logo, the type and name of the report, report brief description and reporting period, and information about the objects for which this report was created
- Summarized data (calculated, summarized report fields)
- Graphical diagram displaying the general report data
- Table with cumulative data
- Table with detailed data

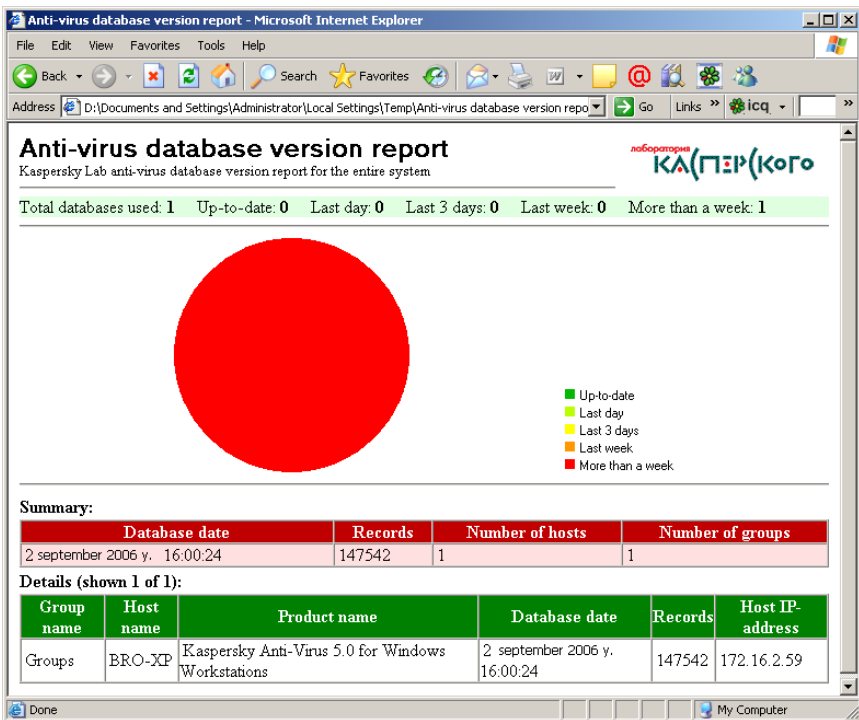


Figure 129. Creating an anti-virus protection level report

## 5.4.4. Generating summary reports on slave Administration Servers

To create a summary report that includes information from slave servers:

1. Select the required report template under the master Administration Server's **Reports** node.
2. Select **Properties** from the popup menu and select the **General** field (see Figure 124).
3. Click **Configure Settings for Administration Server Hierarchy** and in the resulting window (see Figure 130):

Select the desired report template in the **Reports** node on the master Administration Server. In the shortcut menu, click the **Properties** item and, on the **General** tab, set the following parameters:

- check **Include data from slave Kaspersky Administration Servers** checkbox
- specify nesting level for Administration Servers according to their hierarchy using the **Up to nesting level** field.
- enter desired value in the **Data wait timeout (minutes)**. If no information is received from a slave server during the specified time interval, it is considered unreachable (relevant information will be contained in the report).

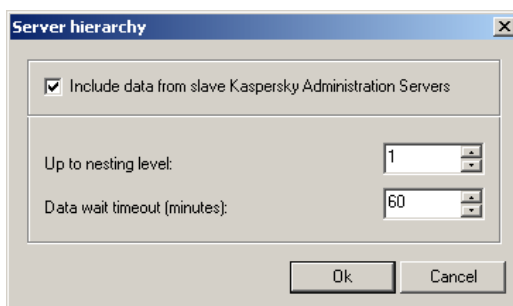


Figure 130. Server hierarchy window

4. Click **Create report**.

As the result, the report will be displayed in your browser window.

## 5.4.5. Restricting the number of records included in the report

To set the maximum number of records included into the report:

select the required report template in the **Reports** node of the main Administration Server. Select the **Properties** command in the shortcut menu and on the **General** tab (see Figure 124) check the **Maximum number of displayed records** box. Enter the required value in the field to the right.

To apply the settings press the **Apply** or **OK** button.

## 5.5. Monitoring Antivirus Protection Status Using System Registry Data

To view client antivirus protection status using data written to the system registry by the Administration Agent:

1. Open client's system registry (for example locally by running **regedit** from **Start / Run**).
2. Select:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\
Components\34\1103\1.0.0.0\Statistics\AVState
```

Antivirus protection status is described by the values of keys listed in Table 1.

Table 1

| Key (Data Type)                              | Value    | Description  |
|--|----------|--|
| <b>Protection_AvInstalled</b><br>(REG_DWORD) | non-zero | Antivirus application installed on host <sup>4</sup> . |
| <b>Protection_AvRunning</b><br>(REG_DWORD)   | non-zero | Permanent protection enabled.                          |

---

<sup>4</sup> An application containing antivirus databases (or threat signature databases) is considered to be an antivirus application.

| Key (Data Type)                           | Value  | Description   |
|---|--|---|
| <b>Protection_HasRtp</b><br>(REG_DWORD)   | non-zero                                       | Permanent protection component installed.   |
| <b>Protection_RtpState</b><br>(REG_DWORD) | 0<br>1<br>2<br>3<br>4<br>5<br>6<br>7<br>8<br>9 | Permanent protection status:<br><br>Unknown;<br>Disabled;<br>Suspended;<br>Starting;<br>Enabled <sup>5</sup> ;<br>Enabled, high level of protection (maximum protection);<br>Enabled, low level of protection (maximum response speed);<br>Enabled, recommended settings;<br>Enabled, user defined settings;<br>Failed. |
| <b>Protection_LastFscan</b><br>(REG_SZ)   | DD-MM-YYYY<br>HH-MM-SS                         | Date and time (in UTC format) of last scan.   |
| <b>Protection_BasesDate</b><br>(REG_SZ)   | DD-MM-YYYY<br>HH-MM-SS                         | Date and time (in UTC format) of antivirus database (threat signature database) publication <sup>6</sup> .  |

---

<sup>5</sup> For applications without detailed antivirus protection status support (Values 5–8).

| Key (Data Type)                   | Value                  | Description  |
|-----------------------------------|------------------------|--|
| Protection_LastConnected (REG_SZ) | DD-MM-YYYY<br>HH-MM-SS | Date and time (in UTC format) of last connection to Administration Server. |

## 5.6. Finding computers

### 5.6.1. Finding computers

To find a computer or a group of computers that match the specified criteria:

Select the **Find computer** item in the shortcut menu of the Administration Server node, the **Network** folder or the administration group. In the window that opens you can specify search criteria in the following tabs: **Network**, **Application**, **Computer status**, **Virus protection** and **External application**.

Using the **Network** tab (see Figure 131) you can specify the following search criteria:

- **Computer name** in the logical network;
- **Computer Windows name**.
- **Computer domain name**: specify the domain to which the client computer belongs.
- **IP-address range**. Specify the start and the end IP addresses of the range.
- **Last connection time range**: specify the time period since the last connection of the client computer with the Administration Server.

---

<sup>6</sup> If several antivirus applications are installed, the date and time of the most recent anti-virus or threat signature databases are specified.

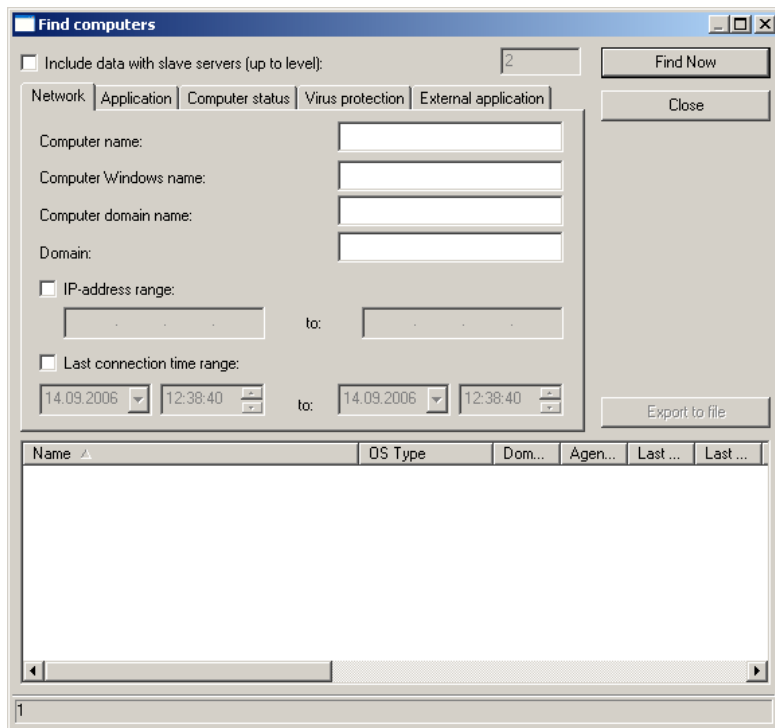


Figure 131. Finding computers. The **Network** tab

Using the **Application** tab (see Figure 132) you can specify the following search criteria:

- **Application name** - specify the name of the application installed on the client computer, by selecting the required value from the drop-down list. The list contains names of only those applications for which management plug-ins are installed on the administrator's workstation.
- **Application version** - specify the version of the application installed on the client computer.
- **Last update time** - specify the time period since the latest update of the anti-virus database and application modules installed on the client computer.
- **Operating system version** - indicate the version of the operating system installed on the computer.

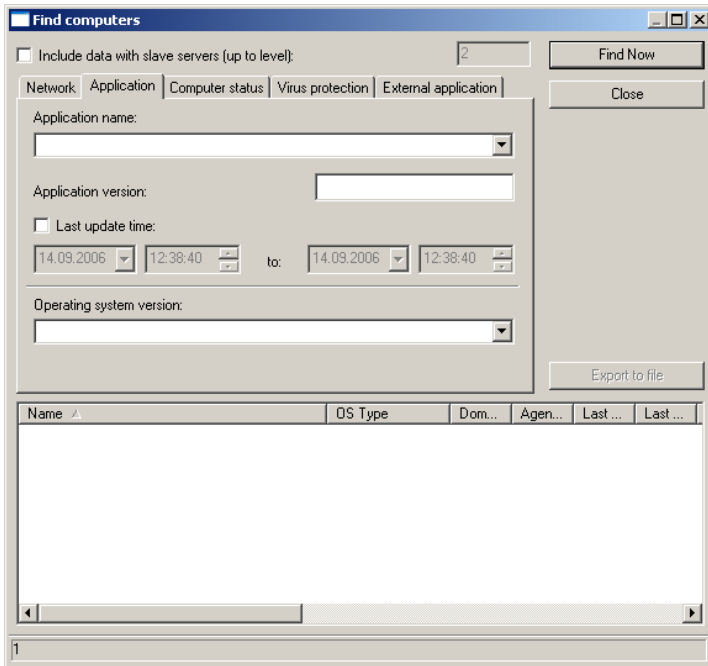


Figure 132. Finding computers. The **Application** tab

Using the **Computer status** tab (see Figure 133) you can specify the following search criteria:

- **Computer status** - select the current computer status from the list: **OK**, **Critical** or **Warning**.
- **Computer status description** - check boxes next to the conditions on which the selected status is assigned to the client computer.
- **RTP status** - select from the list the current status of the real-time anti-virus protection system of the client computer.

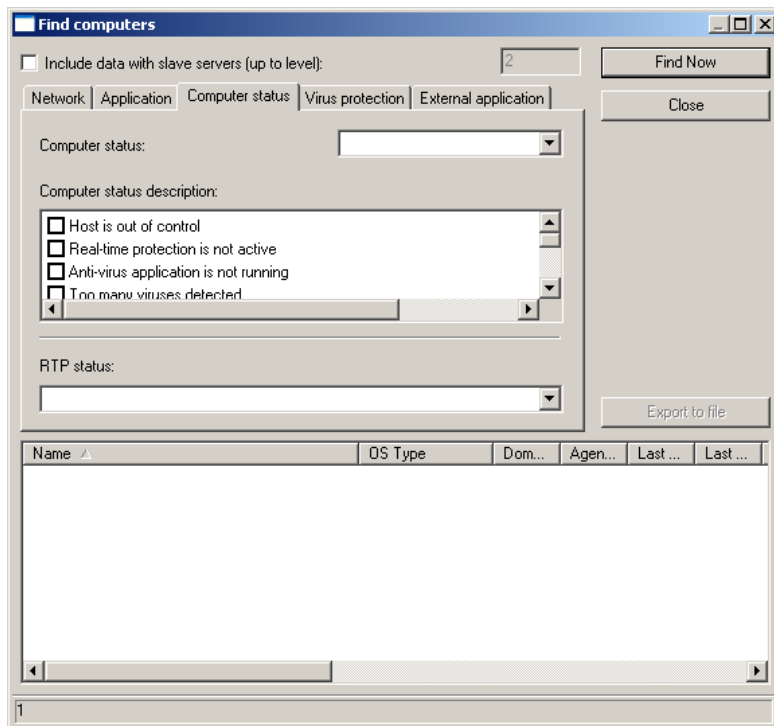


Figure 133. Finding computers. The **Computer status** tab

Using the **Virus protection** tab (see Figure 134) you can specify the following search criteria:

- **Anti-virus database date** - indicate the anti-virus database release date.
- **Anti-virus database records range.**
- **Last full scan time** - indicate the time period during which a full scan of the client computer was last performed.
- **Viruses found.**

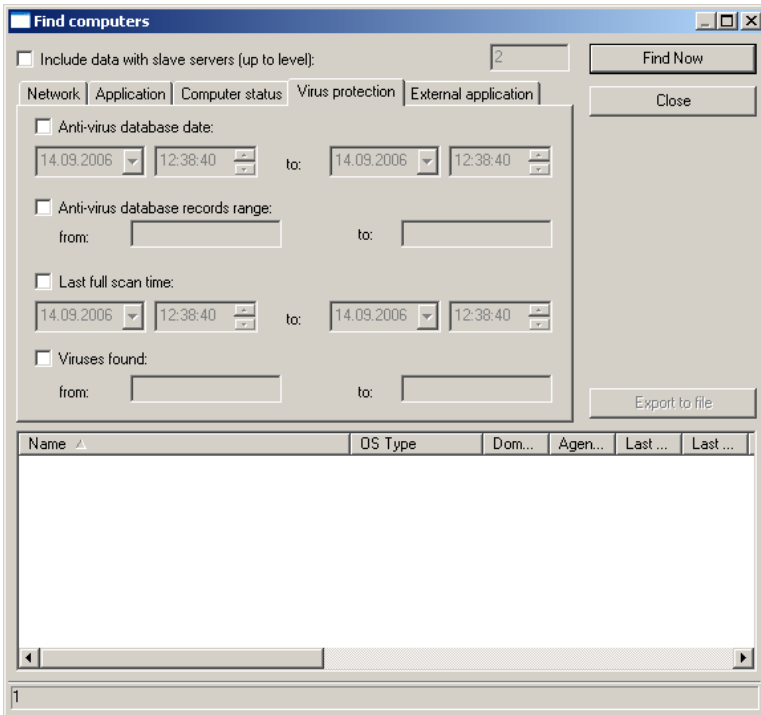


Figure 134. Finding computers. The **Anti-virus protection** tab

Using the **External application** (see Figure 135) select from the list the name of one of the external applications detected within the network.

To allow a search to use information about computers stored on the slave Administration Servers, check the **Use data from the slave servers (up to level)** box, and specify the maximum nesting level to be included in the search.

After you have specified the search criteria, press the **Find now** button and a list of computers matching the specified criteria will be displayed in the bottom part of the window. This list will also contain general information about computers found.

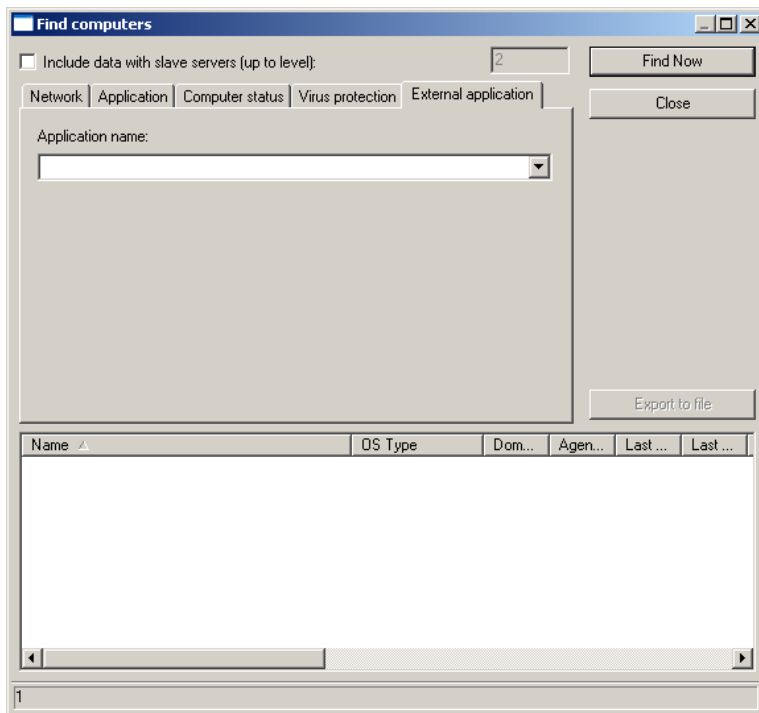


Figure 135. Finding computers. The **External application** tab

## 5.6.2. Saving computer search results in a text file

*To save the search results into a text file,*

press the **Export to file** button in the **Find computers** window (see Figure 134) and specify the file to save the data into in the window that will open.

## 5.7. Computers selections

### 5.7.1. Configuring a computer query

*To create a computer query:*

1. Select the Computer Queries node in the console tree, open the shortcut menu and select the **New/New Query** command or use the analogous item from the **Action** menu.
2. Enter the name for the query in the window that will open. Press the **OK** button to confirm the query's name.

As the result a folder with the name you have specified for the query will appear in the **Computer queries** folder in the console tree. To add computers to the query, configure the query parameters.

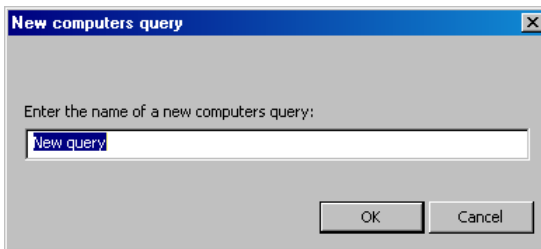


Figure 136. Configuring a computer query

### 5.7.2. Configuring a computer query

*To configure a computer query:*

1. Select the computer query you wish to configure in the console tree or in the results panel and use the **Properties** command in the shortcut menu or the analogous item under the **Action** menu.
2. This will open the query configuration window (see Figure 134) that contains the following tabs: **General**, **Network**, **Application**, **Computer status**, **Virus protection** and **External application**.

Using the **General** tab (see Figure 137) you can modify the query name, and define the computers to be searched, by selecting one of these options:

- **Search in groups and in the network** – the search will be performed for all computers within the network, whether included in the structure of the logical network or not.
- **Search in groups** – search only among client computers of the logical network.
- **Search in the network** – search among the computers not included in the logical network.

To perform a search which includes information about computers stored on the slave Administration Servers, check the **Use data from the slave servers (up to level)** box. After this, specify the maximum nesting level to be included in the search.

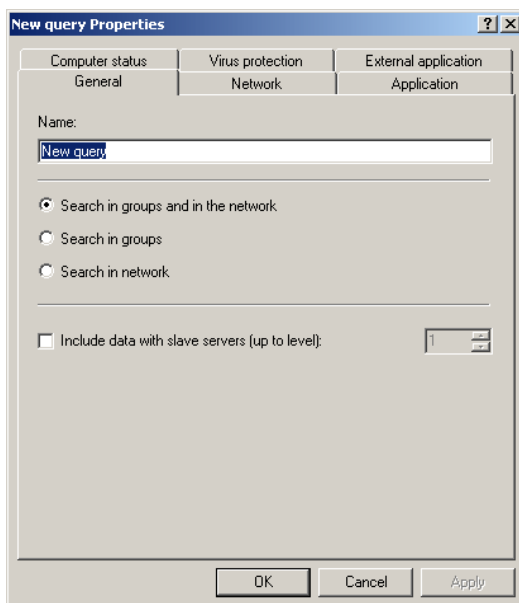


Figure 137. Configuring a computer query.  
The **General** tab

Specify attributes for the computers to be included into the query on the **Network** tab. You can use the following parameters:

- computer's name in the logical network;
- computer's name in the Windows network;
- domain that must include computers;

- the range of IP addresses of the computers; to do this, check the **IP addresses range** box and enter the start and the end IP addresses;
- the time of the last connection of the client computer to the Administration Server; to do this, check the **Last connection time range** box and specify the start and the end date and time of the interval in the **from** and **to** fields.
- the time when new computers appear in the network; to do this, check the **New computers detected during the network polling** and specify period in days in the **Period of detection (days)** field.

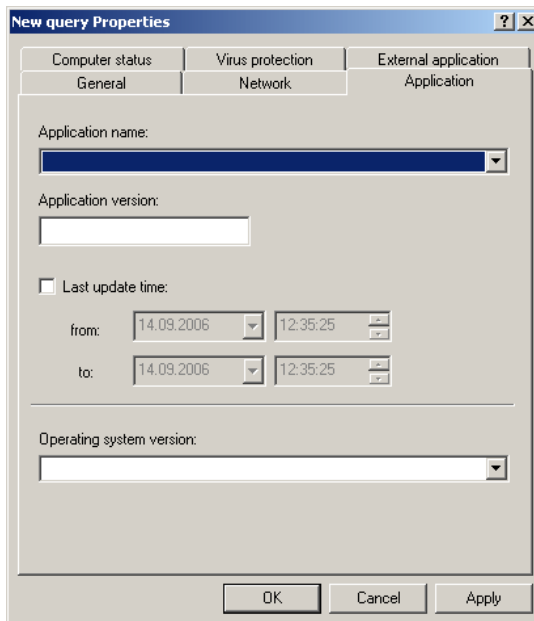
The screenshot shows the 'New query Properties' dialog box with the 'Network' tab selected. The 'IP-address range' checkbox is checked, and the 'Last connection time range' checkbox is also checked. The 'from' and 'to' fields for the last connection time range are both set to 14.09.2006 12:35:05. The 'New computers found during network scan' checkbox is unchecked, and the 'Detection period (days)' is set to 0.

Figure 138. Configuring a computer query.  
The **Network** tab

Specify which Kaspersky Lab application must be installed on computers using the **Applications** tab (see Figure 139). You can use the following parameters:

- **Application name** - select the required value from the drop-down list. The list contains names of only those applications for which management plug-ins are installed on the administrator's workstation.

- **Application version;**
- the time of the last update of the application; to do this, check the **Last update time** box and specify the start and the end date and time of the interval in the **from** and **to** fields;
- version of the operating system installed on the computer.



The screenshot shows a dialog box titled "New query Properties" with three tabs: "Computer status", "Virus protection", and "External application". The "External application" tab is selected, and within it, the "Application" sub-tab is active. The dialog contains the following fields and controls:

- Application name:** A dropdown menu.
- Application version:** A text input field.
- Last update time:** A checkbox.
- from:** Two dropdown menus for date and time, showing "14.09.2006" and "12:35:25".
- to:** Two dropdown menus for date and time, showing "14.09.2006" and "12:35:25".
- Operating system version:** A dropdown menu.
- Buttons for **OK**, **Cancel**, and **Apply** at the bottom.

Figure 139. Configuring a computer query.  
The **Applications** tab

Specify criteria to evaluate the anti-virus protection on the computers which will be included in the query on the **Virus protection** tab. You can specify:

- date of the creation of the anti-virus database used by the applications; to do so, check the **Anti-virus database date** box and specify the time interval matching the date of the anti-virus database release;
- number of records in the anti-virus database used by applications; to do so, check the **Anti-virus database records range** box and specify the minimum and the maximum number of records.
- the time when the full computer scan by one of the Kaspersky Lab's anti-virus applications was last performed; to do so, check

the **Last full scan time** box and specify the time interval during which the scan was performed;

- the number of viruses detected on the computer; to do so, check the **Viruses found** detected and specify the minimum and the maximum possible values for this parameter.

Figure 140. Configuring a computer query.  
The **Anti-virus protection** tab

On the **Computer status** tab (see Figure 141), specify parameters that characterize the status of the computers and the status of the real-time protection performed on computers. To do this:

- select the required value from the Computer status drop-down list: **OK**, **Critical** or **Warning**;
- select the conditions based on which the computer is assigned the status from the **Computer status description** list.
- select the status of the real-time protection running on the computers included in the query from the **RTP status** list.

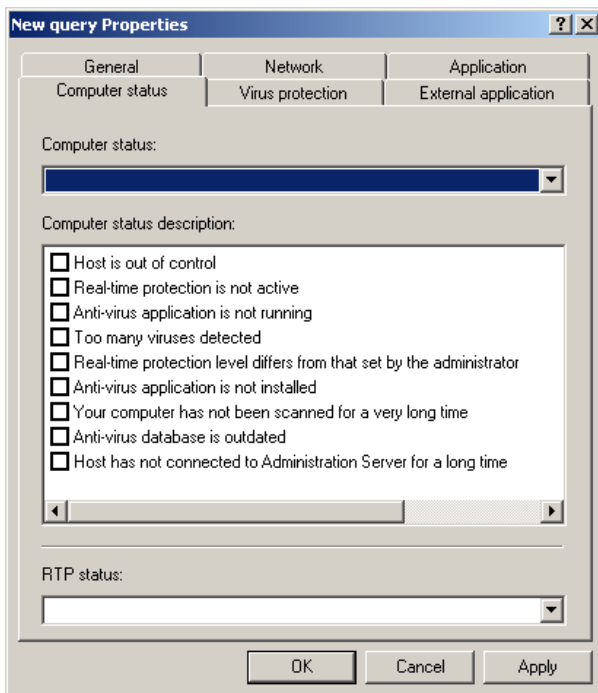


Figure 141. Configuring a computer query  
The **Computer status** tab

On the **External application** (see Figure 141) specify the external application installed on the computer.

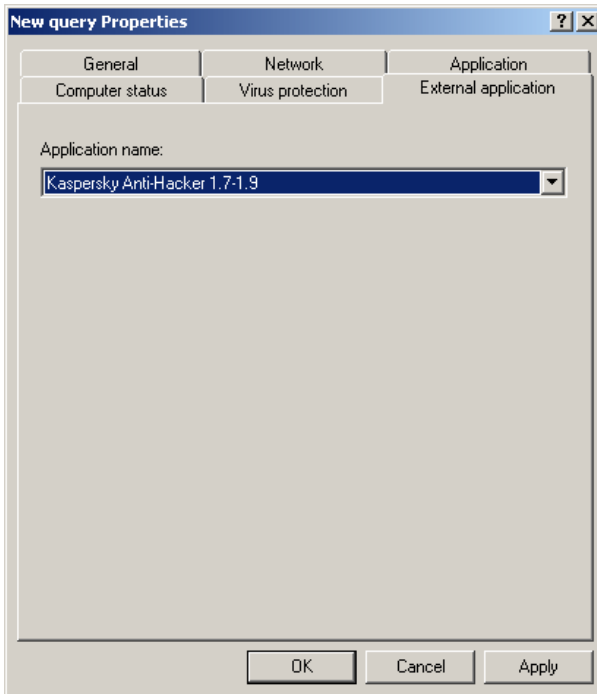


Figure 142. Configuring a computer query  
The **External Application** tab

3. To confirm the changes press the **Apply** or **OK** button.

## 5.8. Tracking virus outbreaks

### 5.8.1. Enabling virus attack detection mechanism

*To ensure that the **Virus attack** event is registered in the logical network and that the notification of this event is issued:*

1. In the console tree, select the node corresponding to the required Administration Server., Open the shortcut menu and select the **Properties** command or use the analogous item from the **Action** menu. This will open the **Properties:<Administration server name>** window.

2. On the **Virus outbreak** tab (see Figure 70) check the boxes next to the names of the required types of antivirus applications, and specify parameter values that determine the threshold of virus activity. Any time that a threshold is exceeded will be considered increased virus activities and will cause the **Virus outbreak** event.
3. On the **Events** tab (see Figure 66), while configuring events with the **Critical event** level, select the **Virus outbreak** event type and indicate the notification settings values.
4. For policies for all anti-virus applications, on the **Events** tab (see Figure 41), while configuring events with the **Critical event** level, select the **Virus found** or **Detection of Virus, Worm, Trojan, and Malware** event type and check the **Save on Administration server for (days)** checkbox under event properties on the **Logging** tab.

The **Virus attack** event cannot be created more than once in 24 hours. You can reset information about the occurrence of such event only by restarting the Administration Server service.

For the purpose of counting **Virus detected** and **Detection of Viruses, Worms, Trojans, and Malware** events only information from the client computers of the main Administration Server is to be taken into account. For each slave Server event **Virus attack** is configured individually.

## 5.8.2. Changing the application policy when a Virus attack event is registered

*To ensure that the current application policy changes once a Virus attack event occurs:*

check the **Activate policy based on an event** box and select the **Virus outbreak** event on the **General** tab (see Figure 37) of the application policy settings configuration window.

## 5.9. Backup copying and restoration of Administration Server data

### 5.9.1. Backup copying of Administration Server data

*To create a backup copy of the Administration Server data:*

- create and launch a global task of data backup copying using the **Administration Console**  
or
- run the **klbackup** utility on the computer where the Administration Server is installed, with the required set of command line parameters. This utility is included in installation file of Kaspersky Administration Kit and after the installation of the Administration Server component it is located in the root of the installation folder.

### 5.9.2. Restoring the Administration Server data from a backup copy

*To restore the Administration Server data*

run the **klbackup** utility on the computer where the Administration Server is installed with the required set of command line parameters.

**The names of the new and the old SQL server must be the same.**

### 5.9.3. Backup data copying task

#### 5.9.3.1. Creating a backup data copying task

*To create an Administration Server backup data copying task:*

1. select the **Global task** 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 launch the task creation wizard (see section 3.2.1 on page 112).

2. Create a global task (see section 3.2.2 on page 122). When creating a task, specify the following values for the parameters:
  - Select **Kaspersky Administration Kit** as the application for which the task is created (see Figure 143). As the task type, select **Backup Administration sever**.

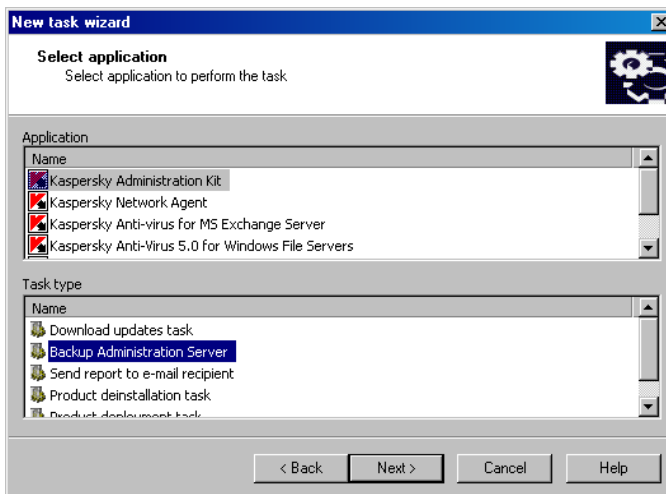


Figure 143. Creating a backup data copying task.  
Selecting application and task type

- Specify on this step of settings configuration (see Figure 144):
  - the backup storage folder, for saving the backup copy of the data; this folder must be write-accessible for both the Administration Server and for the SQL server on which the Administration Server database is installed;
  - password that will be used for encrypting/decrypting the Administration Sever certificate; re-enter the password in the field below;

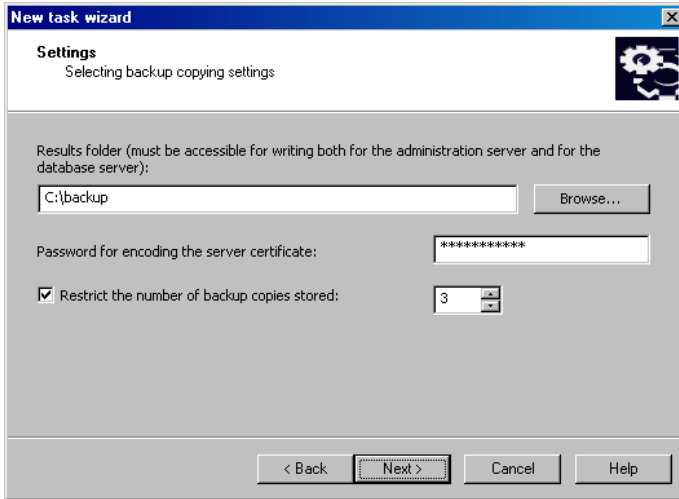


Figure 144. Creating a backup data copying task.  
Configuring the settings

Backup copying of the data is created in the specified folder as a subfolder under a name that reflects the current data and time of the operation in the **klbackup** format as follows: **YYYY-MM-DD # HH-MM-SS** (where **YYYY** - year, **MM** - month, **DD** - day, **HH** - hour, **MM** - minutes, **SS** - seconds). The following information will be saved in this folder:

- information database of the Administration Sever (policy, tasks, application settings, events saved on the Administration Server);
- configuration information about the structure of the logical network and client computers;
- storage of the installation files for deployment of applications (content of the Packages folder);
- Administration Server certificate.
- If required, restrict the number of backup copies that can be simultaneously located in backup storage. To do this, check the **Restrict the number of backup copies stored** box and specify the required number of copies. If the imposed restriction has been met, the previous, older copies stored in the backup storage will be removed.

### 5.9.3.2. Configuring the Administration Server data backup copying task

*To configure the Administration Server data backup copying task:*

1. Select the required tasks for the Global tasks node in the results panel, open the shortcut menu and select the Properties command or use the analogous item in the **Action** menu.
2. In the window that opens, select the **Settings** tab (see Figure 145). This tab displays the same settings that were determined when the task was created:
  - folder for saving the backup data copy;
  - password that will be used for encrypting/decrypting the Administration Server certificate; re-enter the password in the field below;
  - restriction imposed on the number of backup copies.Specify the required values for these settings.
3. To confirm your changes, press the **Apply** or **OK** button.

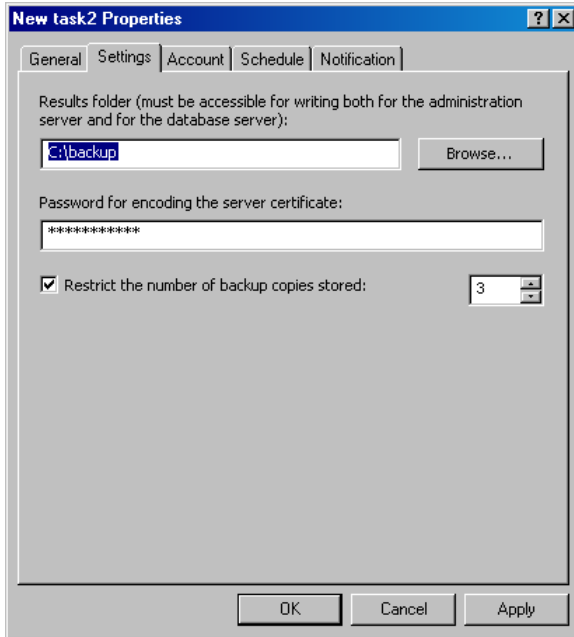


Figure 145. Configuring the backup copying task settings

## 5.9.4. Backup data copying utility

### 5.9.4.1. Creating a backup copy of the Administration Server data manually. The *klbackup* utility

*To create a backup copy of the Administration Server data manually:*

start the **klbackup** utility on the computer where the Administration Server is installed, using the required command line parameters.

Utility command line syntax:

- **klbackup** [-logfile LOGFILE]<sup>7</sup> -path BACKUP\_PATH [-use\_ts] | [-restore] -savecert PASSWORD

Description of the command line parameters:

- **-logfile LOGFILE** - save a report about execution of the task of copying/restoration of the Administration Server data.
- **-path BACKUP\_PATH** - save information in folder **BACKUP\_PATH** for restoring user data from folder **BACKUP\_PATH** (required parameter).

The account of the database server and the **klbackup** utility must have access rights to modify the **BACKUP PATH** folder.

- **-use\_ts** - when saving the data, copy information into the folder under the name that reflects the current date and time of the operation in format **klbackup YYYY-MM-DD # HH-MM-SS** nested into **BACKUP\_PATH** folder. If no modifier is specified, information will be saved into the root of the **BACKUP\_PATH** folder.

When attempting to save information into the folder in which a backup copy already exists, an error message will appear and no update will occur.

The use of modifier **-use\_ts** allows maintaining the archive of the Administration Server data. For example, if folder **C:\KLBackups** was specified using **-path** modifier, then information about the Administration Server status as of June 19, 2006, 11:30:18 will be saved in folder **klbackup 2006-06-19 # 11-30-18**.

- **-restore** - will restore the Administration Server data. Restoration of the data will be performed based on information stored in the **BACKUP\_PATH** folder. If the modifier is missing the backup data will be copied into the **BACKUP\_PATH** folder.
- **-savecert PASSWORD** - save / restore the Administration Server certificate use the password specified in the **PASSWORD** setting for encrypting/decrypting the certificate

---

<sup>7</sup> Entries in square bracket are optional modifiers.

Full restoration of the administration system data requires mandatory saving of the Administration Server certificate. The **PASSWORD** setting must be specified.

When restoring the certificate, the password matching the password provided during backup copying must be provided. If the password is incorrect, the certificate will not be restored.

If, during the restoration of the Administration Server data, the path to the public folder changed, you should verify the execution of tasks in which this folder is used (update, deployment tasks) and, if necessary, change the settings.

### 5.9.4.2. Moving the Administration Server to a different computer

*To move the Administration Server to a different computer:*

1. Create a backup copy of the Administration Server data.
2. Install a new Administration Server.

To simplify moving the logical network, it is desirable that the new server's address matches the old server's address. The address (computer's name in the Windows network or IP address) must be indicated in the Network Agent's settings as part of the parameters used to connect to the Server.

3. Restore the old server's data from the backup copy on the new Administration Server.
4. If the address (computer's name in the Windows network or the IP address) of the new and the old servers do not match, create an **Administration server change** task for the **Groups** group to connect the client computers to the new server.

If the addresses do match, there is no need to create the server change task as the connection will be made using the Server address specified in the settings.

5. Remove the old Administration Server.

### 5.9.4.3. Moving the Administration Server database to a different computer

*To move the Administration Server to a different computer, and change the Administration Server database:*

1. Create a backup copy of the Administration Server data.
2. Install a new SQL server.

To ensure that the information is moved correctly, the database on the new SQL server must have the same collation as the old SQL server being replaced.

3. Install a new Administration Server. The names of the new and the old SQL server must be the same.

To simplify moving the logical network, it is desirable that the new server's address matches the old server's address. Address (computer's name in the Windows network or IP address) must be indicated in the Network Agent's settings as part of the parameters used to connect to the Server.

4. Restore the old server's data from the backup copy on the new Administration Server.
5. If the address (computer's name in the Windows network or the IP address) of the new and the old servers do not match, create an **Administration server change** task for the **Groups** group in order to connect the client computers to the new server.  
  
If the addresses do match, there is no need to create the server change task as the connection will be made automatically.
6. Remove the old Administration Server.

## 5.10. Configuring Integration with Cisco Network Admission Control (NAC)

*To configure a mapping between Cisco NAC statuses and antivirus protection conditions:*

1. In the console tree, select the node corresponding to the desired Administration Server. Open a popup menu and use the **Properties** option or a similar option under the **Action** menu. This will open the **Properties:<Administration Server Name>** dialog.
2. Select the **Cisco NAC** tab (cf. Figure 72).
3. In the upper field select a Cisco NAC status: **Healthy**, **Checkup**, **Quarantine** or **Infected**.
4. Check the antivirus protection conditions mapping to the status in question. If required, modify condition thresholds.
5. Enter the Posture Validation Server port number used to communicate with the Cisco server in the **PVS Port Number Field**
6. To confirm your changes, click **Apply** or **OK**.

---

# APPENDIX A. HOW TO CONTACT TECHNICAL SUPPORT SERVICE

If you encounter any problems while using the application, you may contact the Kaspersky Lab's technical support service.

First of all, try to find a description of your problem and its solution in the documentation or in the **Services / Knowledge base** section of Kaspersky Lab's website at [www.kaspersky.com](http://www.kaspersky.com).

If you have not found a solution for your problem in the documentation and in the online Knowledge base, we recommend that you contact Kaspersky Lab's technical support service.

If you have a problem that must be solved immediately, call phone numbers specified in section on page **Error! Bookmark not defined**. Phone support is provided 24/7 in Russian, English, French and German. Please pay attention that in order to obtain help, you must be registered user and provide to the Technical Support service representative your registration number (if you purchased a retail box version) or information about your order (if you purchased the product via the internet).

*To send a message about problems with the application operation to the Technical Support Service,*

open the Kaspersky Lab's website ([www.kaspersky.com](http://www.kaspersky.com)) and switch to section **Services / Technical Support** section.

On the page that opens fill in the Technical support request form. In the first window of the form provide information about the problem you encountered and the Kaspersky Anti-Virus license details.

- In the **Please choose an appropriate type of your request** field select from the drop-down list the particular problem you have encountered while using Kaspersky Anti-Virus.
- Select **Kaspersky Administration Kit** as the name of Kaspersky Lab's product, and provide a detailed description of the problem you encountered in the **Please describe your request** field.
- Select the registration type of the application running under Kaspersky Administration Kit (for example, Kaspersky Anti-Virus 5.0 for Windows Workstations). To do so, specify **license key** if you purchased the product in the box and installed the license key from a disk, or **online purchase** details if you purchased the application online.

- In the **Serial or order number** field enter the serial number of the application license that you use with Kaspersky Administration Kit. The license number can be found in the license key properties in the **License keys** node.
- Enter your e-mail address in the **E-mail address** field.
- Press the **Next** button.

Provide the following information in the next window:

- Indicate your contact details in the **Contact information** section so that we can contact you in order to help you resolve this problem as soon as possible.
- Enter a special numeric code displayed in the **Protection against automatic registration** field to the left of the code.

After this press the **Send request** button.

---

## APPENDIX B. GLOSSARY

This documentation 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. Groups can include other groups. Group policies and group tasks can be created for each application 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.

**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.

**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 by the Administration Console to the server, or upon data transmission between 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.

**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.

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

**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 the copying of:

- Administration Server database that stores policies, tasks, application settings, and events logged on the Administration Server
- Information about 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 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.

**D**

**Disinfection** – A method of treating infected objects. Disinfection implies either 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 on-demand scanning mode.

**External application** – An anti-virus application by a third-party vendor or a Kaspersky Lab application which does not support administration via Kaspersky Administration Kit.

**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 the default settings of the applications.

**K**

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

**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 who 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 use 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 functionality will be restricted.

**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 Network 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. 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 Microsoft Windows NT/2000/2003/XP, which support this feature, or for computers that are running 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 settings recommended by Kaspersky Lab experts, which ensures the optimal protection of your computer. This level is the default configuration.

**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 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 the 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 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** – A named action performed by a Kaspersky Lab application.

## 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 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 C. 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.

## C.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.

## C.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   | <a href="http://www.kaspersky.com/supportinter.html">Please find the technical support information at http://www.kaspersky.com/supportinter.html</a><br>Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">www.kaspersky.com/helpdesk.html</a> |
| General information | WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a><br><a href="http://www.viruslist.com">http://www.viruslist.com</a><br>Email: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>   |

---

# APPENDIX D. 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](http://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](http://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).