

KASPERSKY LAB

Kaspersky Mobile Security 7.0
Enterprise Edition

ADMINISTRATOR'S
GUIDE

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE
EDITION

Administrator's Guide

© Kaspersky Lab
<http://www.kaspersky.com>

Revision Date: September, 2009

Table of Contents

CHAPTER 1. MANAGEMENT VIA KASPERSKY ADMINISTRATION KIT	4
CHAPTER 2. APPLICATION DEPLOYMENT	7
2.1. Creating an installation package	7
2.2. Installing the application using a remote installation task.....	8
2.3. Installing the application using SMS	19
2.4. Adding device to a group	21
CHAPTER 3. MANAGING POLICIES	24
3.1. Creating a policy	24
3.2. Viewing and editing policy settings	31
3.2.1. Viewing application information.....	32
3.2.2. Viewing results of applying of the policy	33
3.2.3. Configuring settings of application operation event registration.....	34
3.2.4. Configuring anti-virus scan settings	35
3.2.5. Configuring Real-Time Protection operation settings.....	37
3.2.6. Selecting the application bases update source	37
3.2.7. Configuring Anti-Spam settings.....	38
3.2.8. Configuring Anti-Theft settings	40
3.2.9. Configuring additional settings	41
CHAPTER 4. MANAGING APPLICATION OPERATION SETTINGS.....	43
4.1. Viewing application information	44
4.2. Viewing information about anti-virus scan settings	45
4.3. Viewing information about Real-Time protection settings.....	46
4.4. Viewing information about update source	47
4.5. Viewing information about Anti-Spam operation settings	48
4.6. Viewing information about Anti-Theft operation settings.....	49
4.7. Viewing information about additional settings	50
4.8. Viewing key details	51
4.9. Viewing event information	52
APPENDIX A. KASPERSKY LAB.....	54
APPENDIX B. KASPERSKY LAB END USER LICENSE AGREEMENT	56

CHAPTER 1. MANAGEMENT VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit is a system providing a centralized tool for performing major administrative tasks related to the managing of the security system of mobile devices.

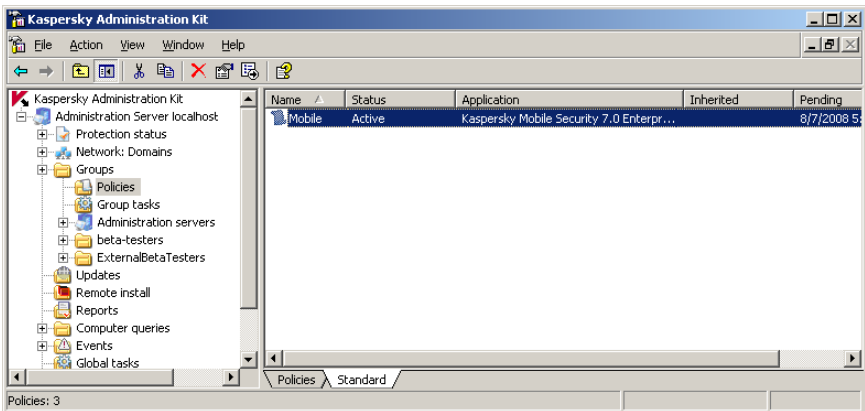


Figure 1. Kaspersky Administration Kit Administration Console

In case of centralized administration via Kaspersky Administration Kit, the Administrator determines the settings of the policies and the application. The protection is built based on these settings.

A peculiarity of centralized administration is the arrangement of mobile devices into groups and managing its settings through creating and defining group policies.

A Policy – is a set of Kaspersky Mobile Security settings in a group of the logical network. Policies are transferred to the mobile device in the course of any type of synchronization of the device with the Administration Server.

Note

To ensure that Kaspersky Administration Kit detects mobile devices, open the **Settings** tab in the Administration Server properties window and check the **Open port for mobile devices** box.

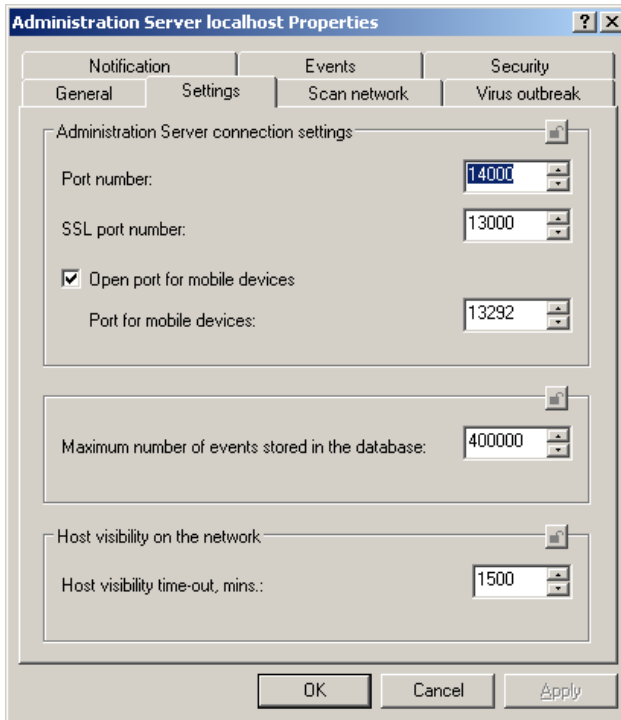


Figure 2. The **Settings** tab

Note!

Mobile devices connect to the Administration Server using the SSL protocol. To establish this type of connection you need a certificate on the Server.

To create a certificate for mobile devices:

1. Open Kaspersky Administration Kit installation folder.
2. Run utility *klmblcrt.exe*.
3. Specify the Administration Server address in the certificate creation wizard window that will open (see Figure 3)

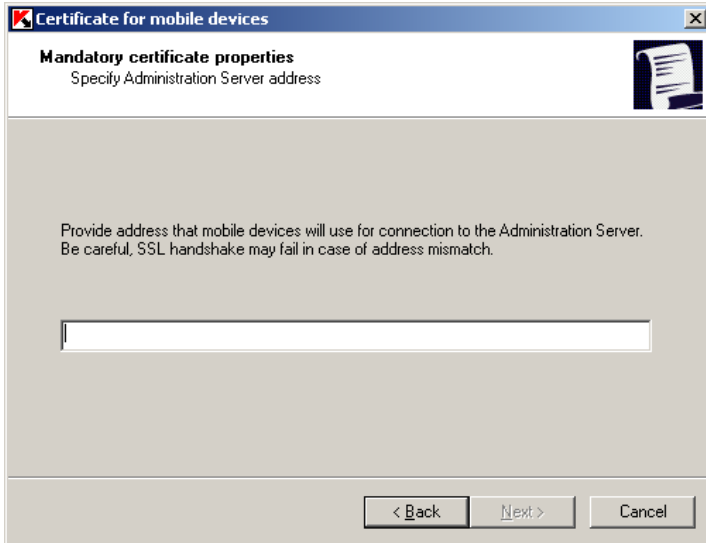


Figure 3. Creating a certificate for mobile devices

4. Follow wizard steps to complete creation of the certificate.

CHAPTER 2. APPLICATION DEPLOYMENT

Note!

Remote installation of Kaspersky Mobile Security is impossible if the Kaspersky Mobile Security administration plugin is not installed on the administrator's workplace. The plugin installation package is included into the Kaspersky Mobile Security distribution kit and can be found in the Plugin folder.

This section describes installation of Kaspersky Mobile security using a remote installation task and using an SMS message.

2.1. Creating an installation package

Remote installation of the application is performed using an installation package.

To create an installation package:

1. Connect to the Administration Server.
2. Select the **Remote install** node in the console tree, open the shortcut menu and select the **New** → **Installation package** command or use the analogous item from the **Action** menu. This will launch the wizard. Follow its instructions.
3. You will be offered to specify the name of the distribution package and to specify the application to be installed during the next step (see Figure 4).
4. Using a drop-down list, select option: **Create installation package for Kaspersky Lab's application**. Using the **Browse** button select the file containing description of the application (this file has extension **.kpd** and is included into the application distribution package). As the result, the fields with the application name and the version number will be filled automatically.

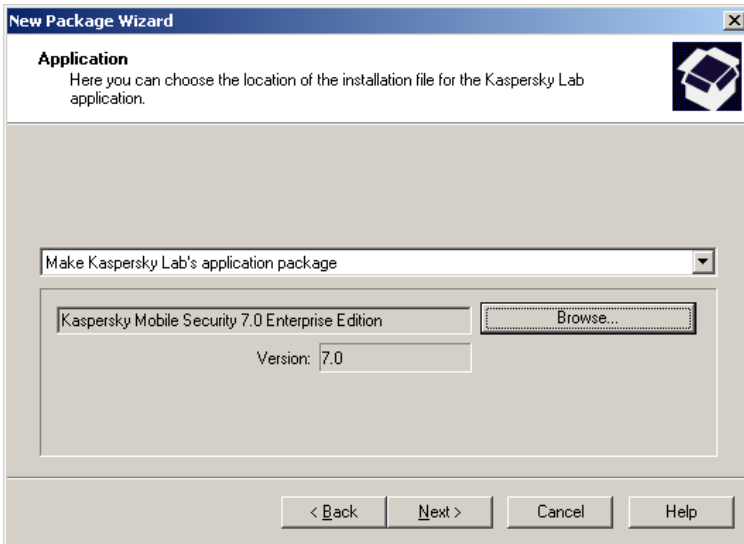


Figure 4. Creating an installation package. Selecting application to be installed

5. After this a set of files required to install the application onto mobile devices will be downloaded to a public folder of the Administration Server.

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

2.2. Installing the application using a remote installation task

Installation of the application using a remote installation task is used when mobile devices are connected to the computers of the logical network. The installation of the application is performed at the moment when the device is connection to the computer.

When performing the task, remote software installation to the client computers can be performed using one of the two methods: the method of *forced installation* or *installation using a start script*.

Forced installation is used to perform a remote installation of software to the specific client computers of the logical network. When the task is launched, the Administration Server copies a set of files required for installation from the public folder to a temporary folder on each client computer and launches the installer on each computer. To ensure success of the forced installation task the Administra-

tion Server must have the privileges of a local administrator on the client computers of the logical network. This method is used for remote application installation on computers running Microsoft Windows NT/2000/2003/XP, which support this feature or on computers running Microsoft Windows 98/Me with the Network Agent installed.

Note!

If the connection between the Administration Server and the client computer is established via Internet or protected with a firewall, public folders cannot be used for data transfer. In this case the files required for application installation must be delivered to the client computer using the Network Agent. Installation of the Network Agent onto such computers is performed locally.

The second method – *installation using a start script* – allows to assign the launch of the remote installation task to a specific user account (or users' accounts). As the result of the execution of this task a record about launching the installer located in the public access folder of the Administration Server will be made in the start script for the specified users. For successful execution of this task the account under which it is run on the Administration Server must have the privilege to modify start scripts in the domain controller database. This privilege is granted to the domain administrator and the task or the entire Administration Server must be started with the rights of such user. As the result, as the user registers with the domain, an attempt will be made to install the application to the client computer from which the user has been registered. This method is recommended for installation Kaspersky Lab's applications onto computers running Microsoft Windows 98/Me.

Note!

For successful execution of the remote installation task using a start script, users for which changes in the scripts are entered, must have the rights of the local administrators on their computers.

Group tasks of remote software installation on client computers are executed only using the forced installation method. When creating a global task, you can select the required method: the method of *forced installation* or *installation using a start script*.

To create a global task of remote installation using a forced installation method:

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

- When selecting the application and determining the task type (see Figure 5) set values **Kaspersky Administration Kit** and **Product deployment task** respectively.
- After this specify the installation package the installation of which will take place during the execution of this task (see Figure 6). Select the package created for this Administration Server or create a new one using the **New** button.

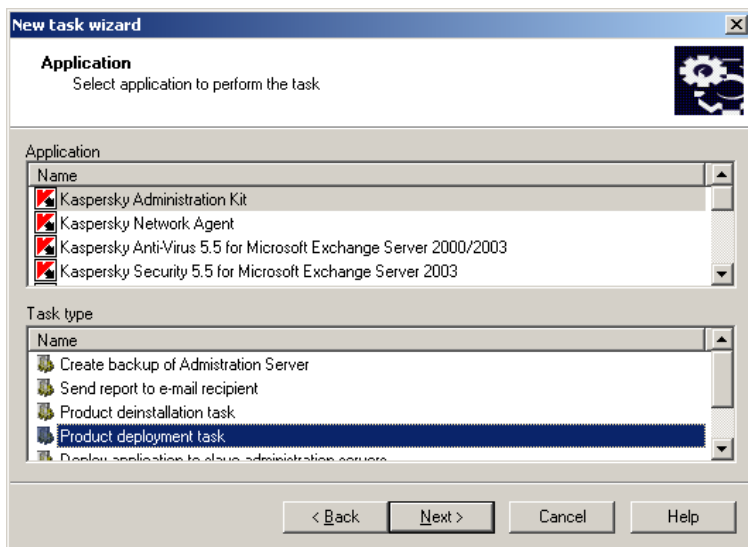


Figure 5. Determining the task type

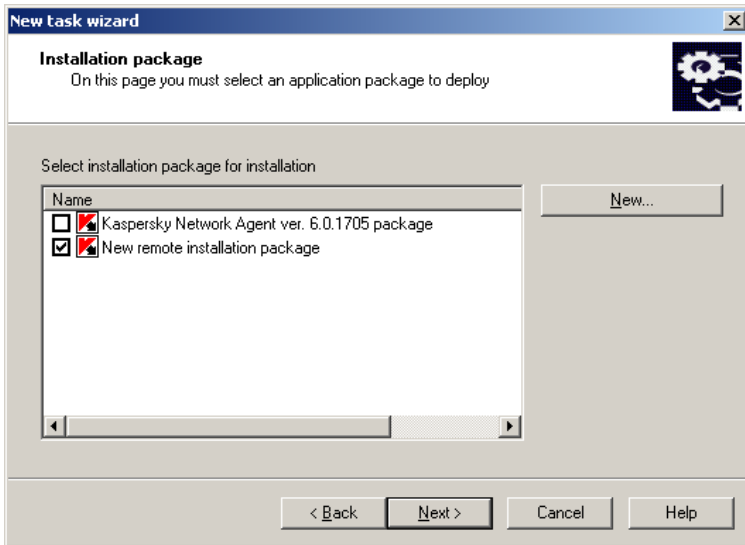


Figure 6. Selecting an installation package to be installed

- At this stage select the **Push install** option (see Figure 7).

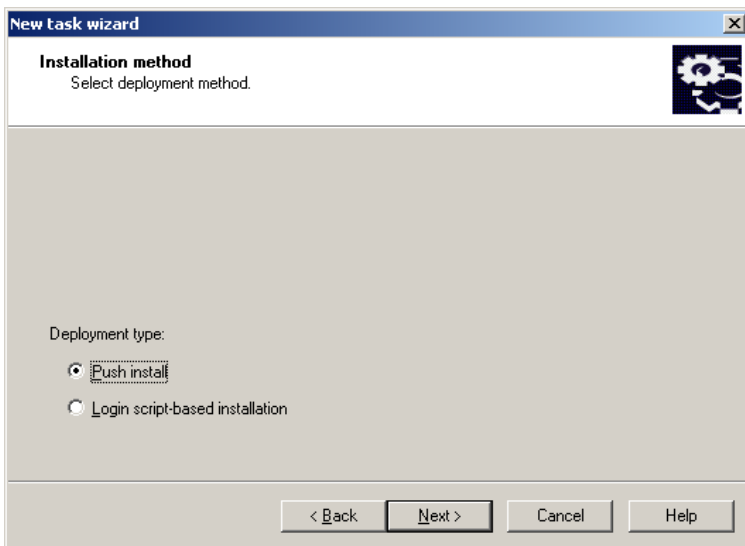


Figure 7. Determining the installation type

7. In this wizard screen (see Figure 8) you will be offered to determine additional installation options:

- Whether you need to reinstall the application if it has already been installed on the computer;
- Check the **Do not install application if it is already installed** box to prevent repeated installation of the application (by default the box is checked). In this case the task will not be started for computers on which the application is already installed locally or as the result of the previously launched remote installation task.

If the box is unchecked, the scheduled remote installation task will be started until the number of installation attempts has been exhausted.

- Define the method to be used to deliver files required to install the application to the client computers;

To do this, do the following in the **Loading installer package** group of fields:

- Check the **Using Microsoft Windows resources from shared folder** box if you want the files needed to remove the program to be copied to the client computers using Windows tools through the public access folder (checked by default). This downloading option is recommended if Network Agent connected to the particular Administration Server is not installed on the computer onto which the installation is being performed.
 - Check the **Using Network Agent** box if you want to deliver the files to client computers through the Administration Agent installed on each of them (checked by default). The Network Agent must be connected to the particular Administration Server.
 - Specify the maximum number of client computers that can download information from the Administration Server in the **The maximum number of simultaneous downloads** field
- Set the number of attempts to install when a task is started by schedule by specifying the value you need in the **Number of attempts** field. Attempts will be repeated if errors occur during the previous installation.

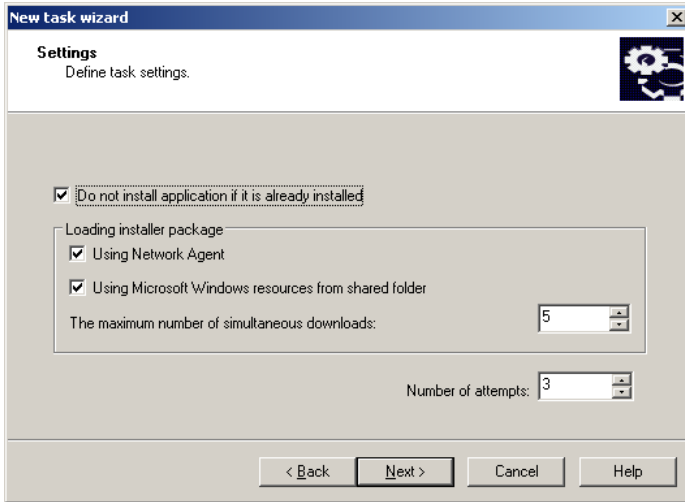


Figure 8. Additional installation options

8. During this step (see Figure 9) you will be offered to install the Network Agent along with the application.

If the Network Agent is not installed on the network computer to which the mobile device will be connected, but you wish to install it, you can include the Network Agent distribution Kit into the application's distribution package.

To do it, check the **Install along with the Network Agent** box and the box next to the name of the required installation package. If it is necessary, create a new installation package using the **Create** button.

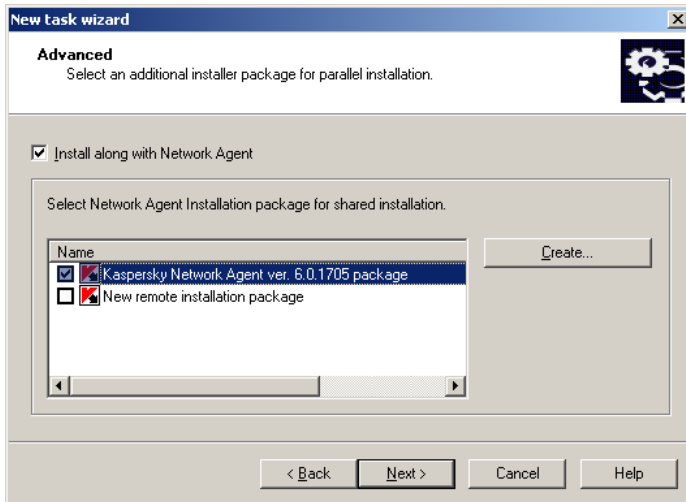


Figure 9. Selecting joint installation with the Network Agent

9. Determine the method to select computers for which the task will be created (see Figure 10):
 - **I want to select computers using Windows Networking.** In this case computers for installation will be selected based on the data obtained by the Administration server by polling the corporate Windows network.
 - **I want to define computer addresses (IP, DNS or NETBIOS) manually.** In this case computers for installation will be selected manually.

If computers are selected based on data obtained by polling Windows network, the list will be created using the wizard screen (see Figure 11) similarly to adding the computers to the logical network (for details see Kaspersky Administration Kit Reference Guide). You can select client computers of the logical network (the **Groups** folder) or computers that are not yet included into its structure (the **Network** folder).

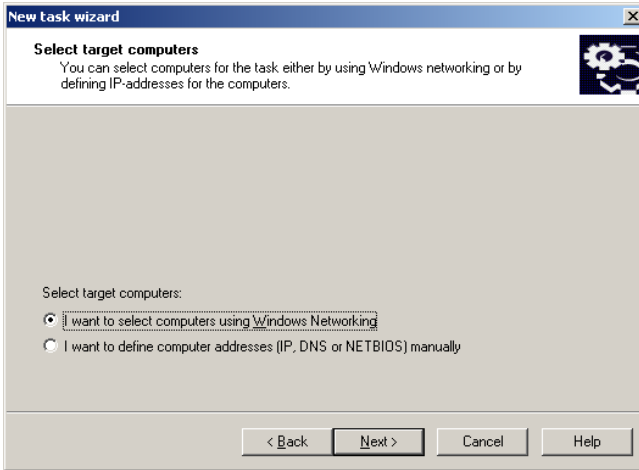


Figure 10. Determining the methods to select client computers

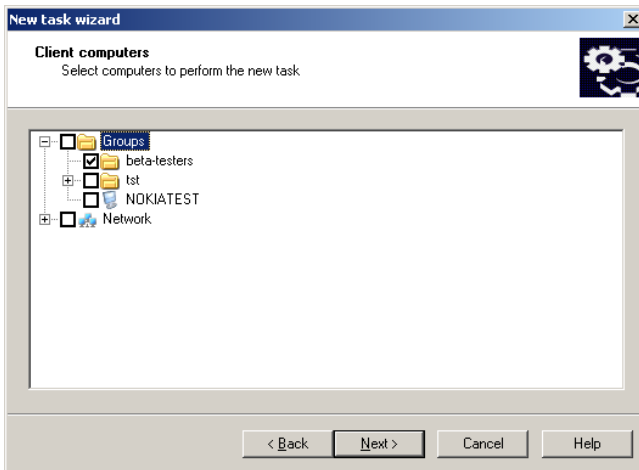


Figure 11. Creating a list of computers for installation based on Windows network data

If computers will be selected manually, the list will be created by entering NetBIOS names or DNS names, IP addresses (or ranges of IP addresses) of the computers, or by importing the list from a `.txt` file in which each address must be entered using a new line (see Figure 12).

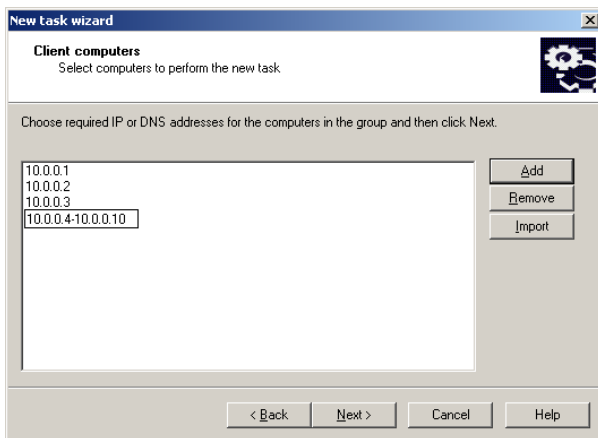


Figure 12. Creating a list of computers for installation based on IP addresses

10. In the next wizard screen specify the account under which the task of remote installation to computers will be executed (see Figure 13).

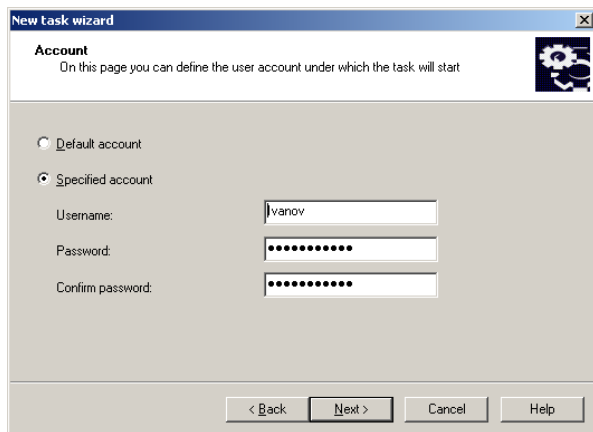


Figure 13. Selecting an account

Note!

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

When installing software on computers belonging to different domains, trust relationship is required between such domains and domains in which the Administration Server is operating.

Select one of the following options:

- **Default account** – if the Administration Server is launched under an account of a domain user and it has the required rights for the installation of the software.
- **Specified account** – if the Administration Server is launched under a system account or if the Administration Server account does not have the right to launch remote installation tasks.

Note!

To perform remote software installation on computers that do not belong to the domain, the remote installation task must be launched under the account of a user who has the administration rights on these computers.

Specify the attributes of the user whose account meets the required conditions in the fields below.

11. Then create the task launch schedule (see Figure 14).

- Select the required task launch mode from the **Scheduled run** drop-down list:
 - **Manually.**
 - **Every N hours.**
 - **Daily.**
 - **Weekly.**
 - **Monthly.**
 - **Once** (in this case the launch of the remote installation task on the computers will be performed only once irrespective of the result of its execution).
 - **Immediately** (immediately after you have created the task, upon the wizard's completion).
 - **On completing another task** (in this case the remote installation task will be launched only after the completion of the specified task).
- Configure the schedule settings using a group of fields matching the selected mode (for details see Kaspersky Administration Kit Reference Guide).

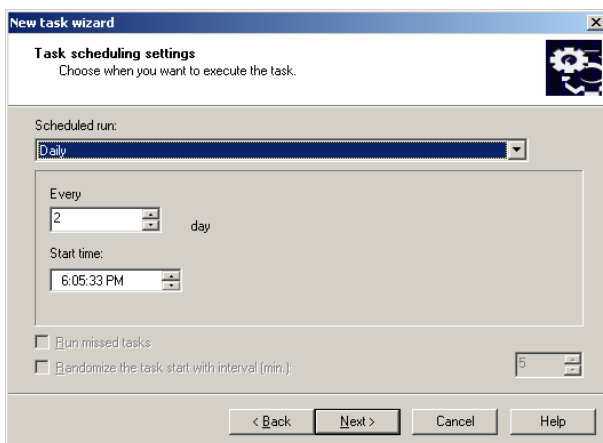


Figure 14. Daily task launch

Upon the completion of the wizard the remote installation task created will be added to the **Global tasks** node and displayed in the result panel.

In order to start the remote installation task.

select the **Global tasks** node in the console tree, select the required installation package, open the shortcut menu and select the **Install** command or use the corresponding item in the **Action** menu.

Once the installation is complete, *kmlisten.exe* application will be run in the background mode; this application will track connection of the mobile devices to the computer. Once a connected device is detected a window will open (see Figure 15) containing a prompt to select a device onto which the application will be installed.

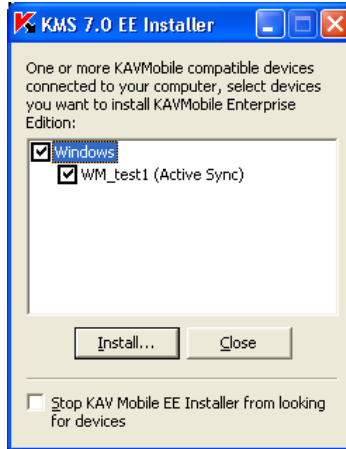


Figure 15. *KMListen.exe* utility window

Press the **Install** button to download the application installation package to the mobile device. Once the download is complete, follow the installation wizard instructions running on the device.

2.3. Installing the application using SMS

Application installation on mobile devices using SMS is used when mobile devices are not connected to the computers of the logical network.

Note!

In order to send an SMS you must have a GSM modem connected to the Administration Server. You will also need Microsoft .NET Framework version 2.0 on the Server. Otherwise sending SMS messages will be impossible

In order to install the application using SMS:

1. Connect to the Administration Server.
2. Select the **Remote install** node in the console tree.
3. Select the **Properties** item from the shortcut menu of the application installation package created.
4. Open the **Settings** tab and press the **SMS Installation** button.

5. In the window that will open (see Figure 16) specify the installation settings:
 - a) Specify the modem connection settings in the **GSM modem** section: port and rate.
 - b) In the **Distribution package URL** field specify a public server on which Kaspersky Mobile Security distribution package is located from which the application will be installed.

For example:

ftp://ftp.domain.com/distrib/KMS7EE/kmsecurity_7_0_15_beta.sis

or:

http://domain_name.ru/distrib/KMS7EE/kmsecurity_ee_wm_sp_7_0_0_49_ru.cab

- c) Create the list of numbers to which SMS message will be sent. In order to do it enter the number in the entry field and press the **Add number** button. The number entered will be added to this list.

To save the list of numbers into a TXT file or load the list from a previously created file, use buttons **Save to file** and **Add from file**.

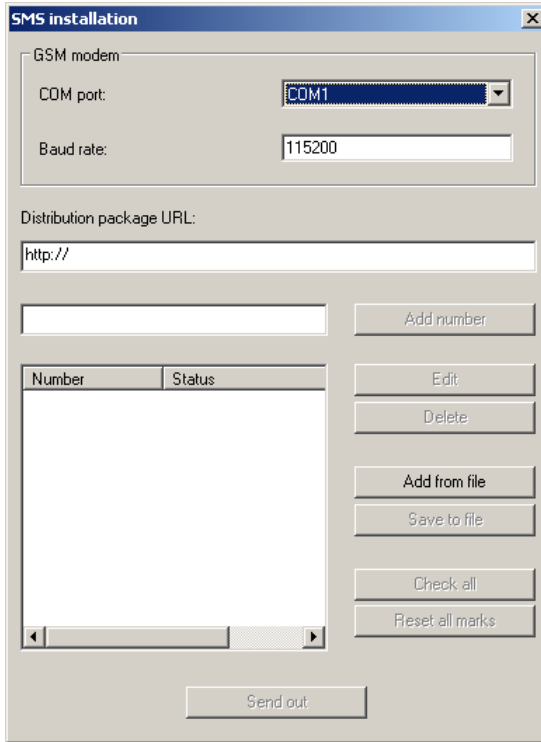


Figure 16. SMS sending settings

6. Press the **Send out** button to send SMS for installation of Kaspersky Mobile Security to the specified numbers.

SMS message containing the URL of the installation package will be sent to the mobile devices whose numbers are found in the list. When you open the URL, the application installation package will be downloaded to the device. Once the download is complete, follow the installation wizard instructions running on the device.

2.4. Adding device to a group

After the installation of Kaspersky Mobile Security, during the network polling all mobile devices will be placed into the domain with the name specified when the installation package was created (by default – **PDAGroup**). The policy created for mobile devices will not be applied.

Note

A group for mobile devices will appear in the **Network** container (in the domain display mode) after the first connection of the mobile device with the Administration service provided that Kaspersky Mobile Security is installed on the device.

To move the mobile device into the administration group open the Administration Console, switch to the **Network** container and select the domain display mode. Expand the **PDAGroup** group in the list of network groups and drag the mobile device into the required administration group.

In order to ensure that the mobile devices are automatically placed into the required group:

1. Open the Administration Console and switch to the **Network** container.
2. Select the **PDAGroup** and open the group properties window using the context menu.
3. Open the **Client computers** tab (see Figure 17).

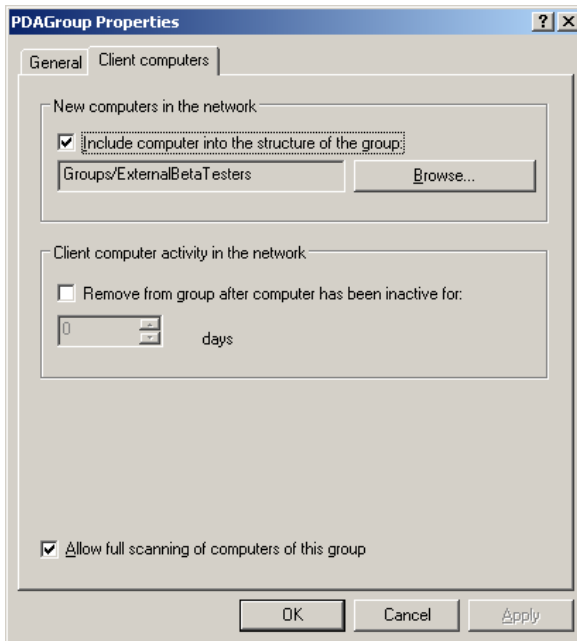


Figure 17. Group properties

4. Check the **Include computer into the structure of the group** box in the **New computers in the network** section.

5. Press the **Browse** button and in the window that will open select the administration group into which mobile devices connected in the future will be placed.
6. Save changes.

CHAPTER 3. MANAGING POLICIES

This section contains information about creation and configuration of policies for Kaspersky Mobile Security 7.0 Enterprise Edition.

The policy is applied to the application in the following cases

- during the device's first connection to the network;
- during subsequent device's connections if the application operation settings or the policy's settings have been modified;
- during synchronization started manually (Kaspersky Mobile Security User's Guide).


3.1. Creating a policy

In order to create a policy, perform the following:

1. Select a group of mobile devices for which you wish to create a policy in the console tree in the **Groups** folder.
2. Select the **Policies** folder included into the selected group, open the shortcut menu and use the **New→Policy** command.

The policy creation utility is designed as a Microsoft Windows wizard and includes a sequence of windows (steps) navigated using the **Back** and **Next** buttons and completed using the **Finish** button. To exit the wizard at any step, press the **Cancel** button.

Note!

On each step of a policy creation the settings you specified can be saved using the  button. If the lock on the button is closed, then when policy is used later on the mobile devices, only values specified by the policy being created will apply

Step 1. Entering general information about the policy

The first wizard's step is introductory. In the first wizard's screen you must specify the name of the policy (the **Name** field), in the second screen - select applica-

tion **Kaspersky Mobile Security 7.0 Enterprise Edition** from the **Application name** drop-down list. In order to apply the policy settings immediately after their creation, check the **Active Policy** box in the **Policy status** block in the third screen.

Step 2. Defining background anti-virus scan settings

At this stage you will have to determine the mobile device anti-virus scan settings: the scan scope and the scan launch schedule.

In the **Scan settings** section (see Figure 18) you can select the scan scope by selecting file types which will be scanned and determine whether attempts will be made to disinfect an infected object:

- **Scan executable files only** - scan executable program files only.
- **Archives** - scan files packed into archives.
- **Try to disinfect infected objects** – attempt to disinfect infected objects encountered. Not every object can be disinfected.

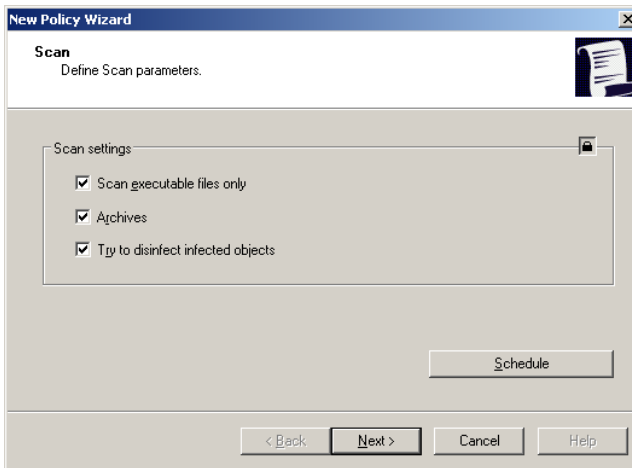


Figure 18. Configuring the anti-virus protection settings

In order to configure a schedule according to which the on-demand scan will be performed press the **Schedule** button. This will open a dialog box in which you should specify the scan frequency:

- **Manually** – the action will be started manually by the user.
- **Daily** – the action will be performed daily. Specify the time for the scan to run in the **Startup time** group of fields.

- **Weekly** – the action will be performed on a certain weekday. In the **Startup time** group of fields specify the time for the action to be performed and select a weekday on which the on-demand scan will run.

Step 3. Configuring Real-Time Protection settings

During this step you will determine the operation settings of Real-Time protection of the mobile device's file system and memory.

Check the **Enable Real-Time Protection** box (see Figure 19) to make the application scan all programs run and files opened by the user.

You can use the **Scan settings** section in order to select the scan scope through selecting the file types to be scanned:

- **Scan executable files only** - scan executable program files only.

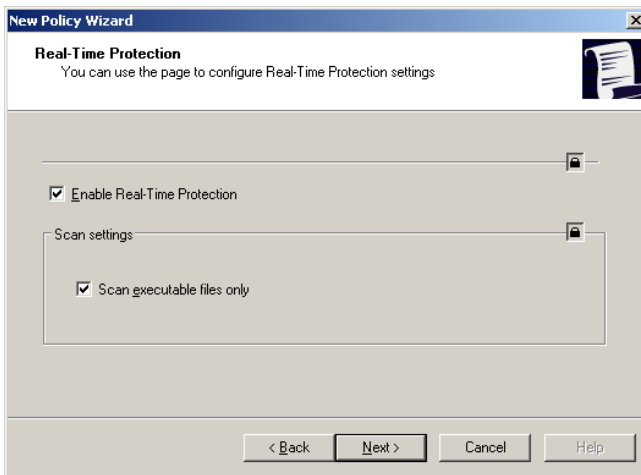


Figure 19. Configuring Real-Time Protection settings

Step 4. Selecting an update source

During this step you will determine the update source and configure the schedule according to which updates will be performed.

Using the **Update source** section (see Figure 20) specify the addresses of the server from which the updates will be made.

To ensure that the updates are performed from the Kaspersky Lab's update servers leave the **Update server** field blank.

When using a different resource for updates, specify the address of the update source in the **Update source** section. It must be a full URL of file *mobile.xml*.

For example, <http://domain.com/index/mobile.xml>.

Note!

The folder structure in the update source must be identical to the corresponding structure of the Kaspersky Lab's update sever.

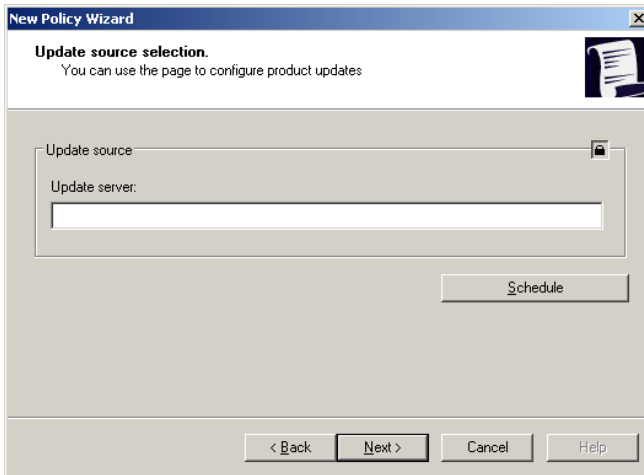


Figure 20. Selecting an update source

Additionally, you can create an update launch schedule. In order to do this, use the **Schedule** button. This will open a dialog box in which you should specify the update frequency:

- **Manual** – the action will be started manually by the user.
- **Daily** – the action will be performed daily. Specify the time for the update to run in the **Startup time** group of fields.
- **Weekly** – the action will be performed on a certain weekday. In the **Startup time** group of fields specify the time for the action to be performed and select a weekday on which the update will run.

Step 5. Configuring Anti-Spam settings

During this step you can configure Anti-Spam module settings (see Figure 21).

Select the Anti-Spam operation mode in the **Anti-Spam protection** section:

- **Disabled.** Anti-Spam is disabled.
- **Only messages from the white list are delivered.** In this mode Anti-Spam passes messages matching the “white list” criteria. All other messages will be blocked.
- **Only messages from the black list are blocked.** In this mode Anti-Spam blocks receipt of messages matching the “black list” criteria. All other messages will be passed.
- **Standard.** In this mode Anti-Spam filters incoming messages using the “black” and the “white” lists. Once a message is received from a phone number not found in either of the lists, Anti-Spam will notify the user and will offer to block or allow receipt of the message and to add this phone number to the “white” or “black” list.

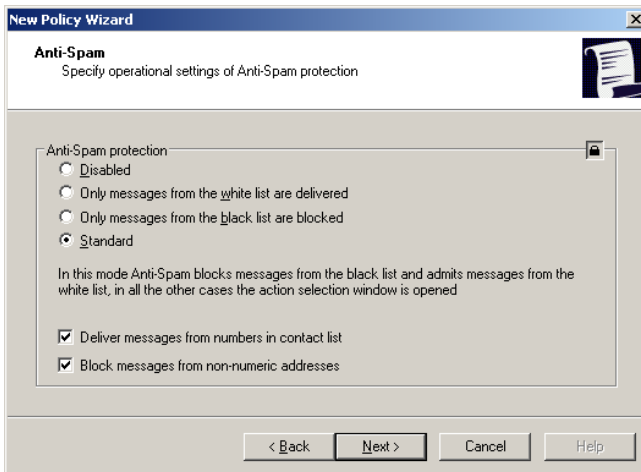


Figure 21. Configuring Anti-Spam settings

Check the **Deliver messages from numbers in the contact list** to ensure that Anti-Spam passes messages from numbers from the contact lists.

Check the **Block messages from non-numeric addresses** box so that Anti-Spam would block receipt of messages from non-numeric numbers.

Step 6. Configuring additional settings

During this step you can specify the Firewall module protection level and the synchronization period with the Administration Server.

Specify the Firewall module protection level in the **Firewall** section (see Figure 22). Firewall ensures mobile device protection on one of the following levels:

- **Disabled.** Firewall disabled.
- **Low level.** Firewall blocks all incoming connections; any outgoing connections are allowed.
- **Medium level.** Firewall blocks all incoming connections; outgoing connections are allowed using ports HTTP/HTTPS/SMTP/IMAP/SSH/POP3.
- **High level.** Firewall blocks any network activities except connections with the Administration Server and updates of the application bases.

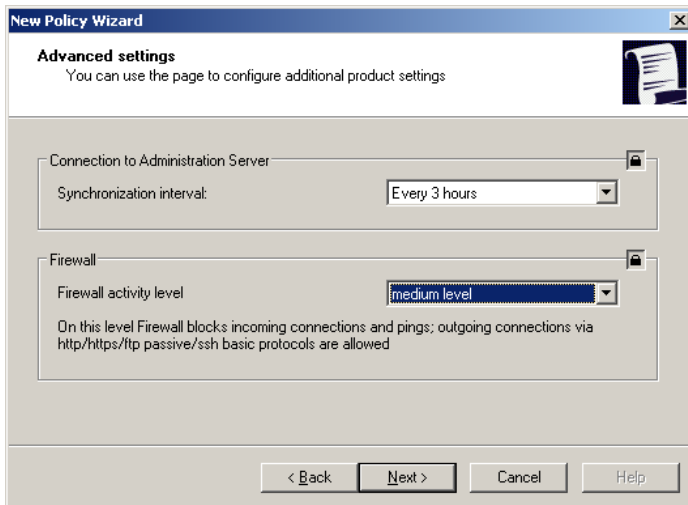


Figure 22. Additional application settings

Specify the synchronization frequency by selecting the required value from the **Synchronization interval** drop-down list in the **Connection to Administration Server** block. By default the mobile device will initiate an attempt to connect to the Administration Server every 6 hours.


Step 7. Selecting a key file

At this step you can specify a key file used to activate Kaspersky Mobile Security.

Press the **Modify** button and select the key file in the window that will open. Then the following information about the key will be displayed in the wizard window:

- number;
- key type;
- License expiration date.
- License restrictions.


Note!

To make sure that the file key is downloaded to mobile devices you must confirm your selection using button . Otherwise Kaspersky Mobile Security will not be activated.

Step 8. Completing creation of the policy

The last screen of the wizard informs about the successful completion of the policy creation process (see Figure 23).

Upon the completion of the wizard policies for Kaspersky Mobile Security 7.0 Enterprise Edition will be added to the **Policies** folder of the corresponding group and displayed in the result pane.

You can edit settings of the created policy and impose restrictions on modification of its settings using the  button for each group of settings. A mobile device user cannot modify settings locked as described above. The policy will be applied to mobile devices at the time of the first synchronization of the client with the server immediately after the mobile device has been added to the administration group.

You can copy or move policies from one group to another or delete them using standard shortcut commands **Copy / Paste**, **Cut / Paste** and **Delete** or analogous items from the **Action** menu.

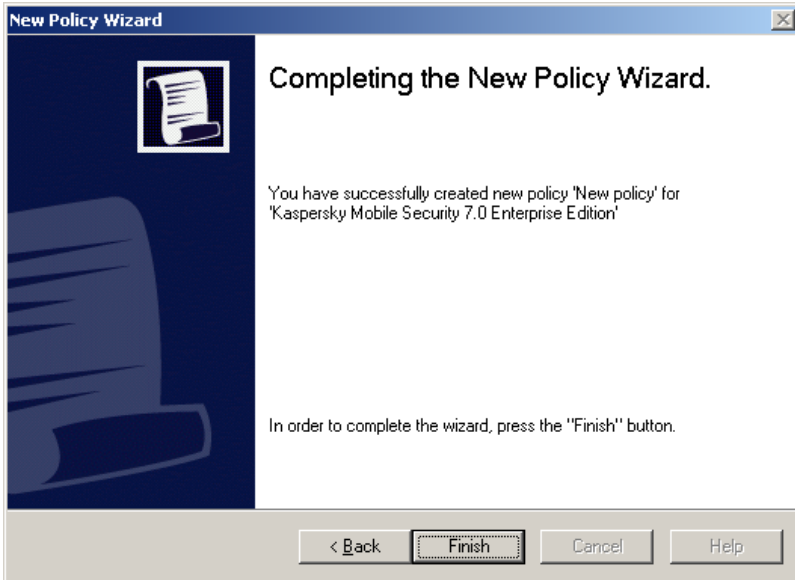


Figure 23. Completing creation of the policy

3.2. Viewing and editing policy settings

At the editing stage you can modify the policy, ban modification of the settings in the policies of nested groups, in the application and task settings.


1. Select a group to which mobile devices belong from the console tree in the **Groups** folder for which you wish to edit the settings.
2. Select the **Policies** folder included into this group; all policies created for this group will be displayed in the result plane.
3. Select the required policy for **Kaspersky Mobile Security 7.0 Enterprise Edition** in the list of policies (the name of the application is indicated in the **Application** field).
4. Select the **Properties** command in the shortcut menu of the selected policy.

An application policies settings configuration dialog box containing several tables will open.

The **General**, **Enforcement** and **Events** are standard tabs for the Kaspersky Administration Kit application (details see Kaspersky Administration Kit Administrator's Guide).

The rest of the tabs contain Kaspersky Mobile Security 7.0 Enterprise Edition settings configuration controls. Description of each tab is provided below.

Note

When editing the policy settings use button  in order to lock the policy data entered. Later the mobile device user will not be able to edit policy settings locked as described above.

3.2.1. Viewing application information

The following information about the policy is displayed in the **General** tab (see Figure 24): policy name, name of the application for which it is created, date and time of the policy creation, date and time of its last modification.

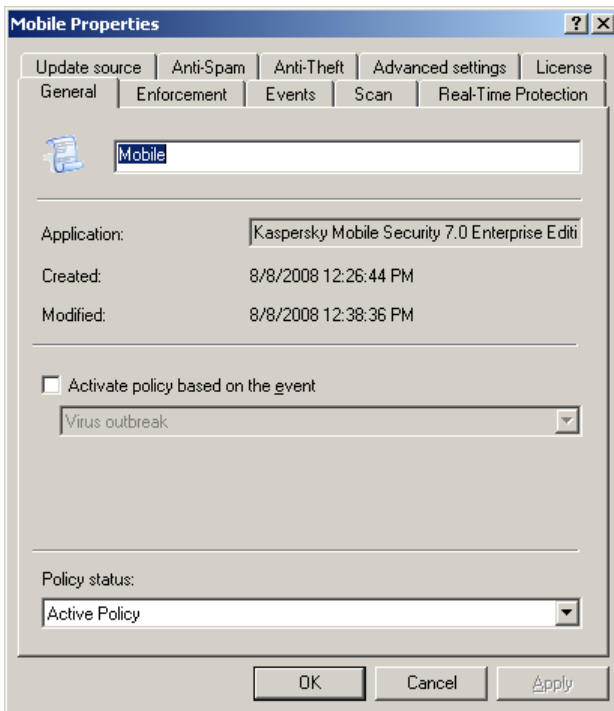


Figure 24. The **General** tab

Using this window you can modify the policy name, activate or deactivate it and configure activation of the policy when a certain event occurs.

3.2.2. Viewing results of applying of the policy

The **Enforcement** tab (see Figure 25) contains general information about the use of a policy on mobile devices of a group and indicates the number of devices on which:

- the policy is not determined;
- executed;
- not yet executed;
- could not be executed due to an error.

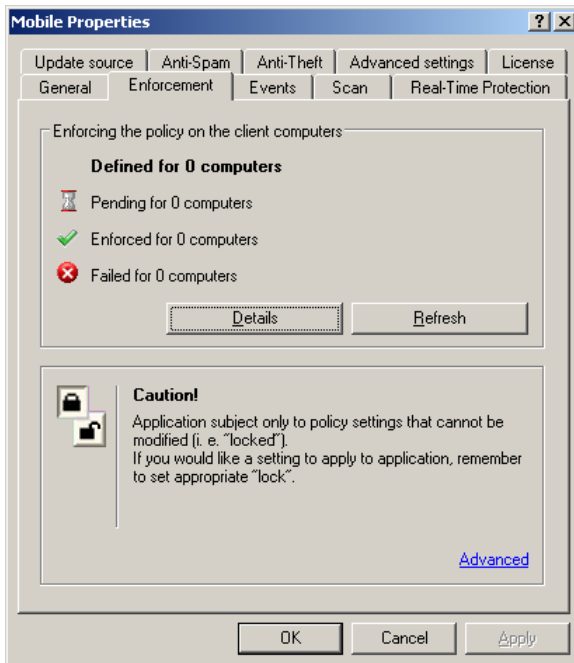


Figure 25. The **Enforcement** tab

You can view details about the results of the use of the policy on each client computer in the group in the window that opens by pressing the **Details** button (for details see Kaspersky Administration Kit 6.0 Administrator's Guide).

3.2.3. Configuring settings of application operation event registration

In the course of its operation Kaspersky Mobile Security generates a certain set of events. Each event has a characteristic that reflects its severity level. There are four severity levels: critical event, functional failure, warning and informational message.

Events of the same type may be of different importance level depending on the situation in which such events occurred.

The **Events** tab (see Figure 26) displays the types of events occurring in the application's operation and logged into the report as well as the location of the report and the mode of the notification of the administrator and other users.

To view the types of events, select the required severity level from the **Severity Level** drop-down list. Types of events for the selected level will be displayed in the information field located below.

For each event you can configure whether it will be logged into the report and whether the administrator will notified about it.

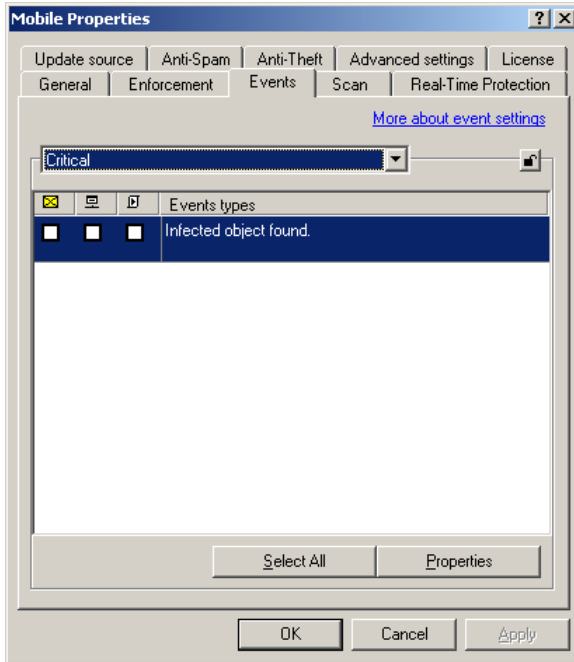


Figure 26. The **Events** tab

For a detailed description of other settings on the **Events** tab refer to the Kaspersky Administration Kit 6.0 Administrator's Guide.

3.2.4. Configuring anti-virus scan settings

The **Scan** tab (see Figure 27) determines the on-demand settings: scan scope, actions to be performed with the infected objects and the schedule according to which the scan will be run.

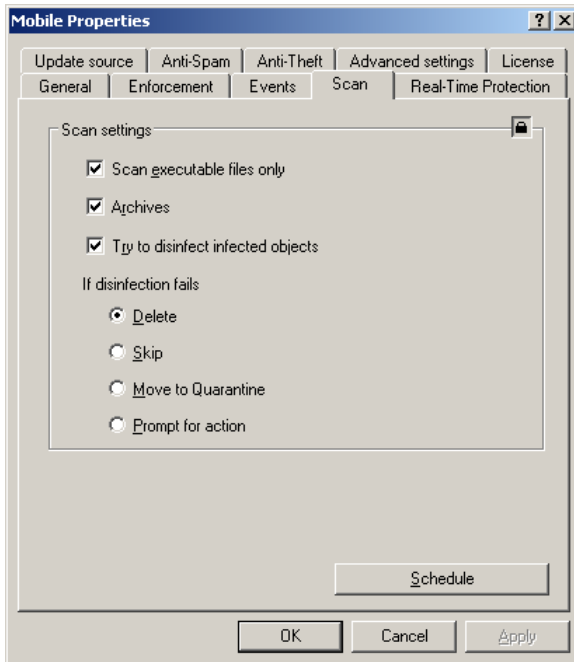


Figure 27. The **Scan** tab

Specify the action to be performed once an infected object is detected in the **Scan settings** section.

- **Delete.**
- **Skip** - leave infected objects detected intact.
- **Move to Quarantine** - move infected objects detected into the quarantine folder.
- **Prompt for action** - display a message about a virus detection on the screen with a suggestion to delete, quarantine or leave the infected object intact.

If the **Try to disinfect infected objects** setting is selected, then the selected action will be performed only if the object could not be disinfected.

Other settings are similar to those described above in section 3.1 on page 24.

3.2.5. Configuring Real-Time Protection operation settings

The **Real-Time Protection** tab (see Figure 28) determines the Real-Time protection settings: scan scope, actions to be performed with infected objects.

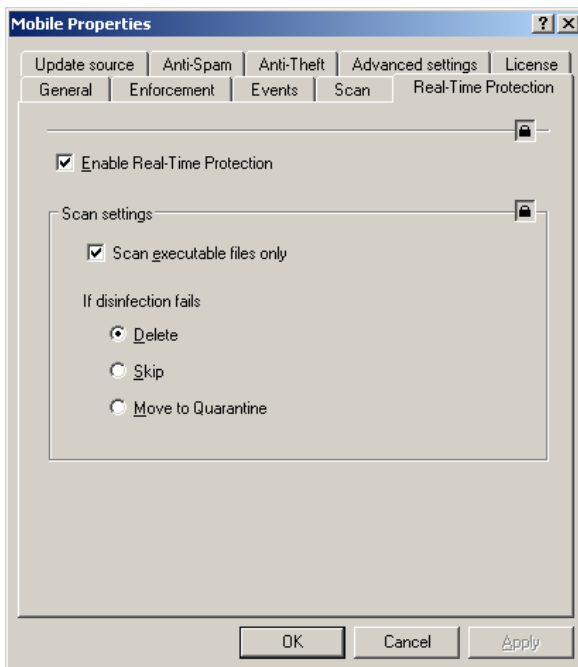


Figure 28. The **Real-Time Protection** tab

3.2.6. Selecting the application bases update source

The **Update source** tab (see Figure 29) indicates the update source from which anti-virus bases updates will be downloaded. This tab is also used to create the update launch schedule.

To ensure that the updates are performed from the Kaspersky Lab's update servers leave the **Update server** field blank.

When using a different resource for updates, specify the address of the update source in the **Update source** section. It must be a full URL of file *mobile.xml*.

For example, <http://domain.com/index/mobile.xml>.

Note!

The folder structure in the update source must be identical to the corresponding structure of the Kaspersky Lab's update sever.

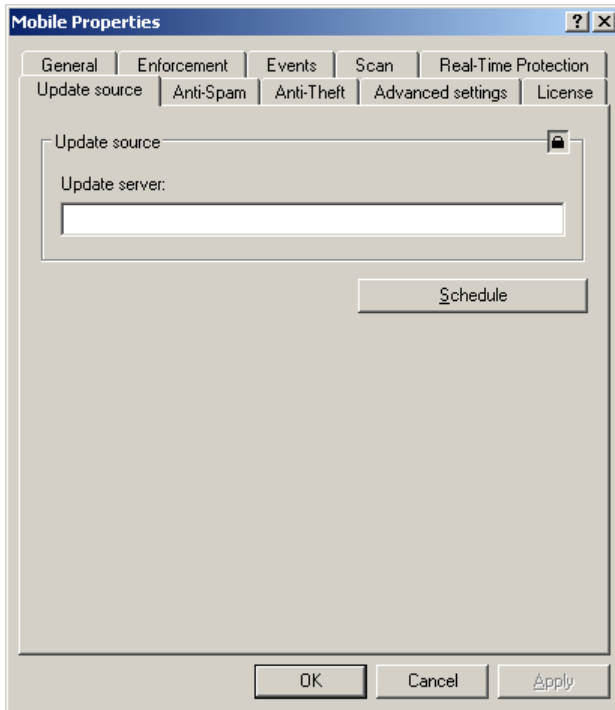


Figure 29. The **Update source** tab

3.2.7. Configuring Anti-Spam settings

The **Anti-Spam** tab (see Figure 30) is used to configure anti-spam settings.

Select Anti-Spam operation mode in the **Anti-Spam** section:

- **Disabled** – disables Anti-Spam.

- **Only messages from the white list are delivered** – Anti-Spam checks messages against the white list. If the sender’s number or the text of the message is found in the list, Anti-Spam will pass such message.
- **Only messages from the black list are blocked** – Anti-Spam checks messages against the black list. If the sender’s number or the text of the message is found in the list, Anti-Spam will block such message.
- **Standard** – Anti-Spam blocks messages from the black list, passes message from the white list; in all other cases a window opens where the device user can select the action to be performed with the message.

Check the **Deliver messages from numbers in contact list** to ensure that Anti-Spam passes messages from numbers from the contact lists.

Check the **Block messages from non-numeric addresses** box so that Anti-Spam would block receipt of messages from non-numeric numbers.

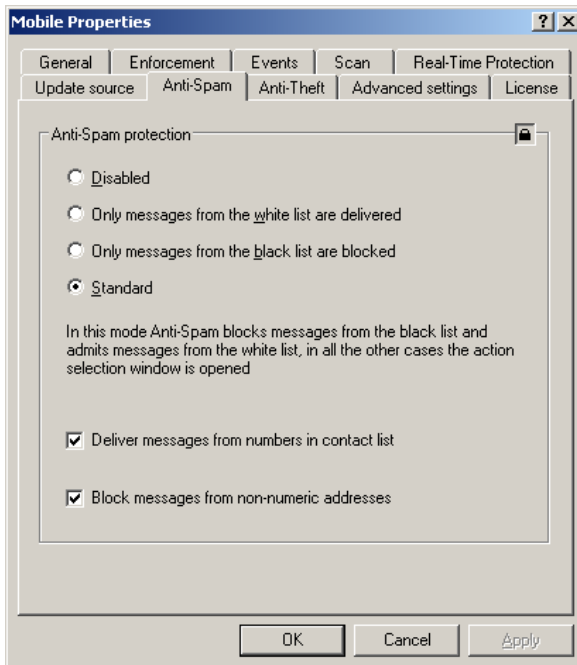


Figure 30. The **Anti-Spam** tab

3.2.8. Configuring Anti-Theft settings

The Anti-Thief module (section **Anti-Theft** (see Figure 31) is used to configure the Anti-Theft module settings that protects data stored on the mobile device against unauthorized access to it in case the device was lost or stolen.

Check the **Enable the SMS-Clean mode** box to enable the SMS-Clean function. This function allows erasing user's personal data (contacts, messages, files, data from the memory card, network settings). To use the SMS-Clean function, send an SMS containing text "clean:code" to the device.

Press the **Configure** button and in the window that will open select the categories of information that can be deleted using the SMS-Clean function:

- **Delete contacts** – deletion of the phonebook.
- **Delete messages** – deletion of messages.
- **Delete documents** – deletion of personal data.
- **Delete data from memory card** - deletion of files from the memory card.
- **Delete network settings and access points configuration** – deletion of personal network settings.

Check the **Enable the SMS-Block mode** box to enable the SMS-Block function. This function allows unblocking of the device. You can unblock it only after you have entered the password. To unblock the device using the SMS-Block function, send an SMS message containing text: «block:code» to the device.

Check the **Enable the SIM Watch mode** box to enable the SMS-Watch function. This function allows to send to the specified numbers a new phone number and to block the stolen device if the SIM card was replaced in such stolen device.

Press the **Configure** button and in the window that will open configure SMS-Clean function's settings. In the **Main phone** and **Additional phone** specify phone numbers to which an SMS message containing a new phone number will be sent if the SIM card is replaced with a new one. Additionally, using the corresponding box you can enable the device blocking function if the SIM card is replaced.

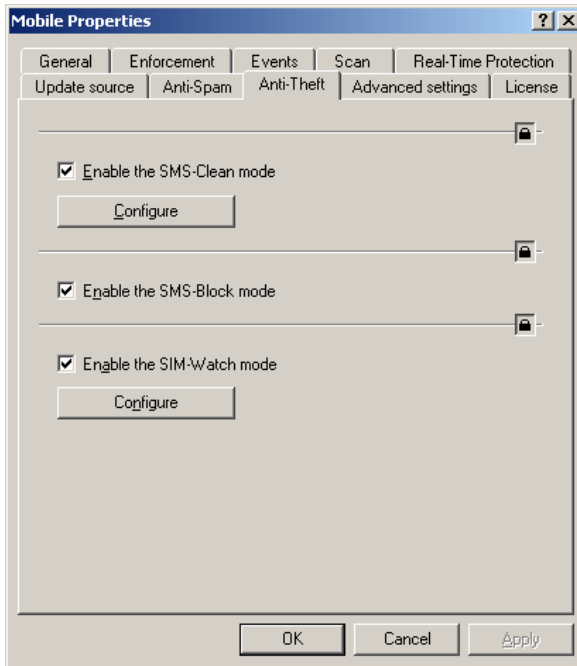


Figure 31. The **Anti-Theft** tab

3.2.9. Configuring additional settings

The **Advanced settings** tab (see Figure 32) is used to set the Firewall protection level and to determine the Administration Server synchronization period.

Specify the synchronization frequency by selecting the required value from the **Synchronization interval** drop-down list in the **Connection to Administration Server** block.

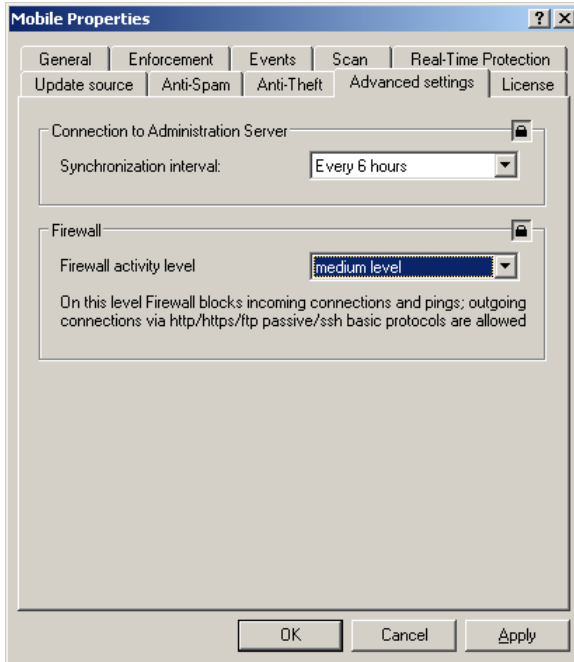


Figure 32. **Advanced settings**

Select the Firewall protection level in the **Firewall** section.

- **Disabled** – disables the Firewall operation.
- **Low level** - Firewall blocks all incoming connections; any outgoing connections are allowed.
- **Medium level** - Firewall blocks all incoming connections; outgoing connections are allowed using ports HTTP/HTTPS/SMTP/IMAP/SSH/POP3.
- **Highest level** - Firewall blocks any network activities except connections with the Administration Server and updates of the application bases.

CHAPTER 4. MANAGING APPLICATION OPERATION SETTINGS

Using the application settings you can modify the settings of Kaspersky Mobile Security operation for individual mobile devices. You can modify only those settings that are not blocked by the policy (for more details see section 3.1 on page 24).

In order to modify the application operation settings:

1. Select the folder with the group name to which the mobile device belongs in the **Groups** folder.
2. Select the device for which you wish to modify the application operation settings in the results pane. Select the **Properties** command in the shortcut menu or in the **Action** menu.
3. As the result a dialog box **Properties: Computer name** will be opened in the main application window. Select the **Applications** tab (see Figure 33).

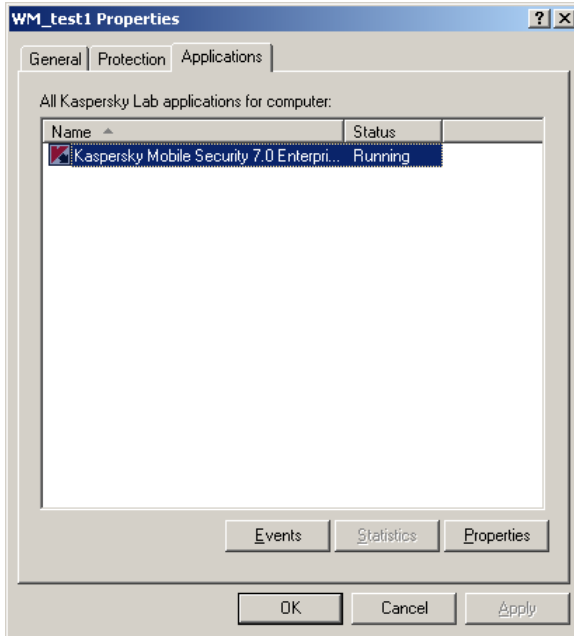


Figure 33. Mobile device properties viewing window.
The **Applications** tab

4. Select application **Kaspersky Mobile Security 7.0 Enterprise Edition**. The bottom left-hand part of the window the following buttons:
 - **Events** – view the list of application operation events occurred in the mobile device and registered on the Administration Server.
 - **Statistics** – view statistical information about the applications' operation.
 - **Properties** – configure the application in the **Kaspersky Mobile Security 7.0 Enterprise Edition application properties** window.

4.1. Viewing application information

Using the **General** tab (see Figure 34) you can view information about Kaspersky Mobile Security 7.0 Enterprise Edition application.

The top part of the window displays the name of the installed application, version information, installation release, current state (whether the application is running on the mobile device) and the information on the application bases status.

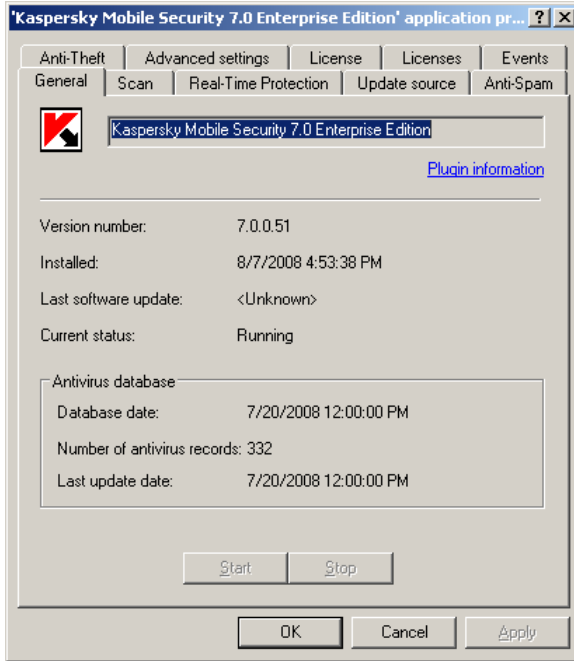


Figure 34. Application settings configuration window.
The **General** tab

4.2. Viewing information about anti-virus scan settings

Using the **Scan** tab (see Figure 35) you can view and modify the on-demand scan settings: scan scope, actions to be performed with the infected objects and the schedule according to which the scan will be run.

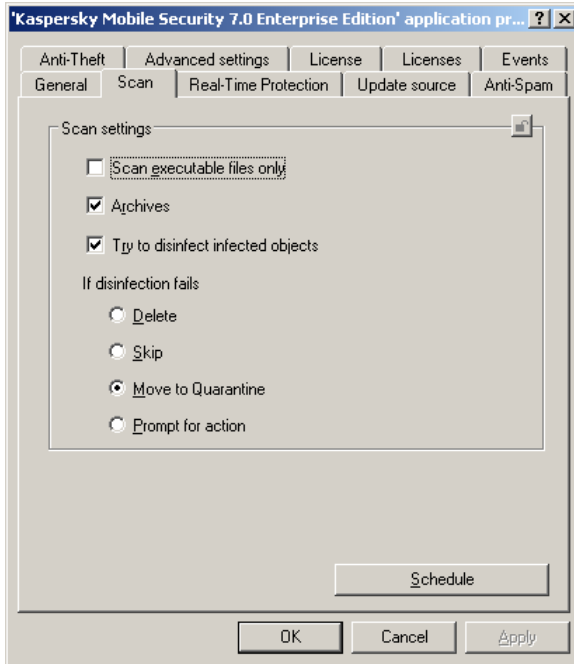


Figure 35. The **Scan** tab

4.3. Viewing information about Real-Time protection settings

Using the **Real-Time Protection** tab (see Figure 36) you can view and modify the real-time protection settings: scan scope and actions to be performed with infected objects.

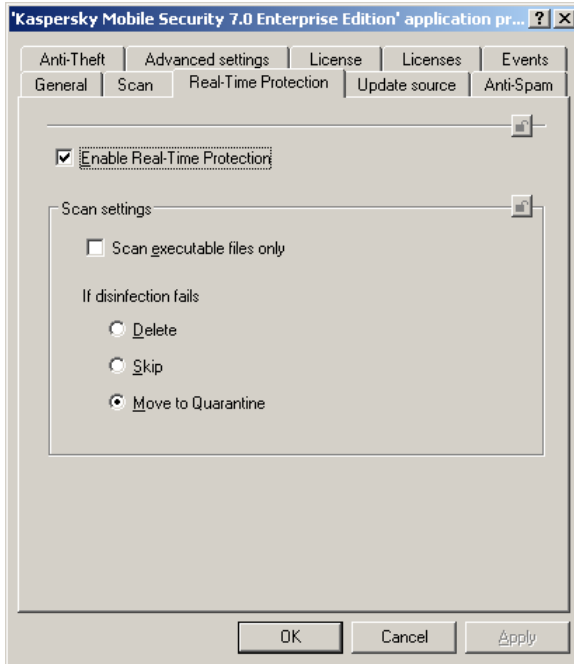


Figure 36. The **Real-Time Protection** tab

4.4. Viewing information about update source

Using the **Update source** tab (see Figure 37) you can view information and modify update downloading settings for the particular mobile device.

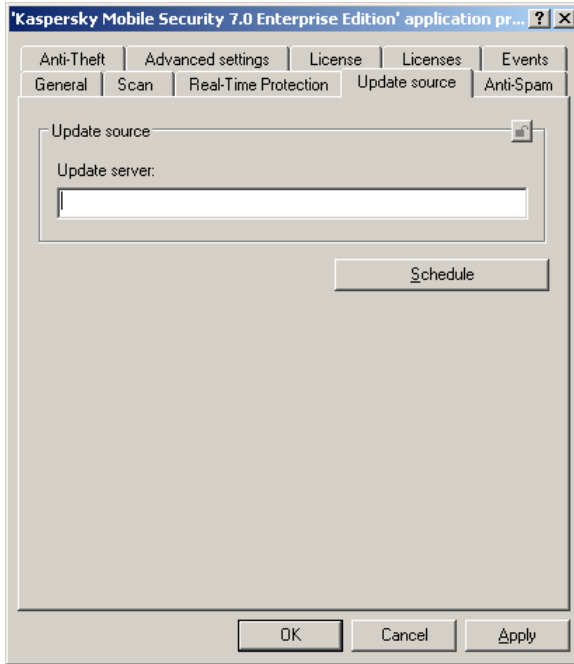


Figure 37. The **Update source** tab

4.5. Viewing information about Anti-Spam operation settings

Using the **Anti-Spam** tab (see Figure 38) you can view and modify the settings of the anti-spam protection of your mobile device.

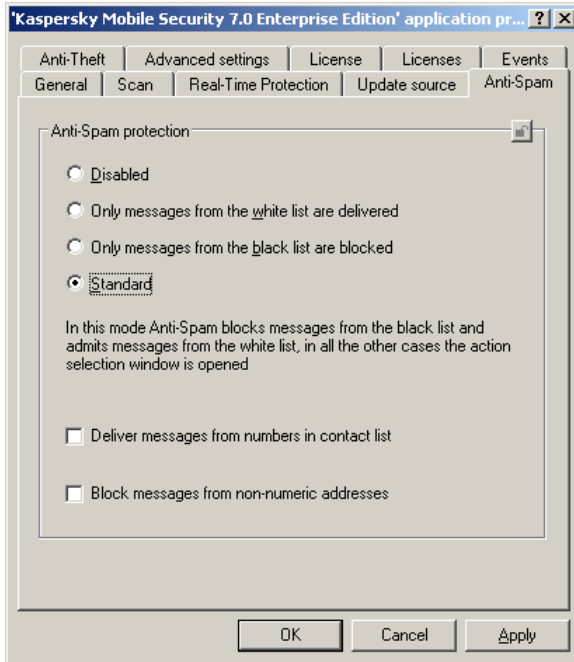


Figure 38. The **Anti-Spam** tab

4.6. Viewing information about Anti-Theft operation settings

Using the **Anti-Theft** tab (see Figure 39) you can view and modify the Anti-Theft operation settings. You can:

- enable module functions: SMS-Clean, SMS-Block, SIM Watch;
- configure the settings of the Anti-Theft function using the **Configure** buttons in the corresponding sections.

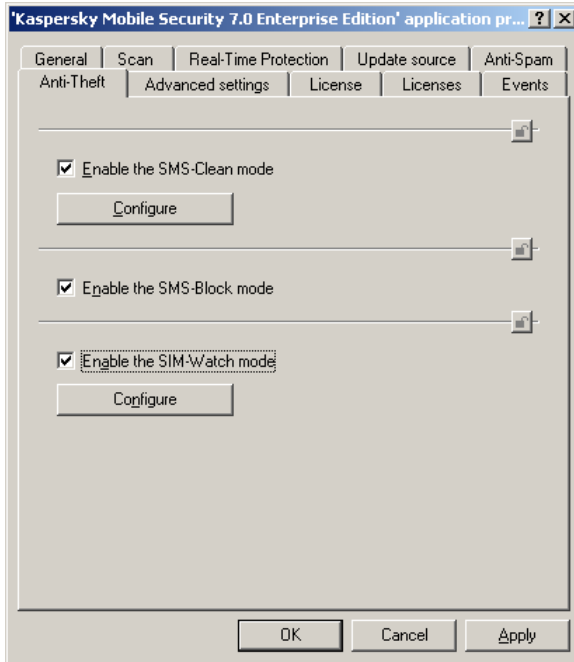


Figure 39. The **Anti-Theft** tab

4.7. Viewing information about additional settings

Using the **Advanced settings** tab (see Figure 40) you can view information and enter changes into the Firewall operation settings and change the frequency of connection with the Administration Server.

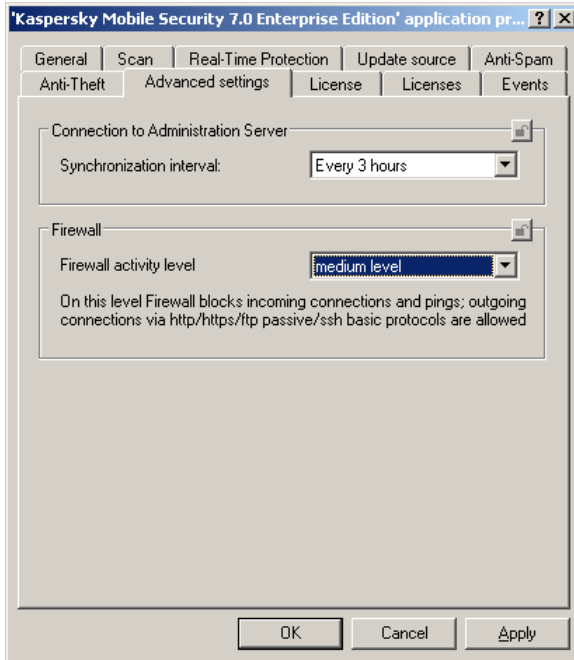
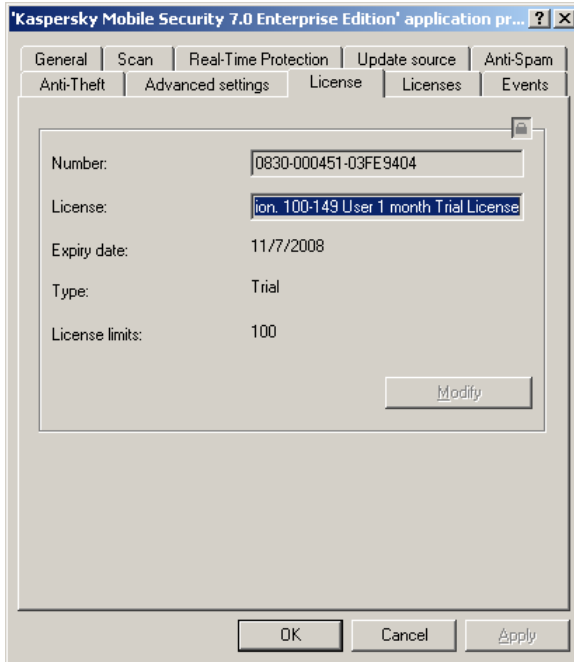


Figure 40. The **Advanced settings** tab

4.8. Viewing key details

The **License** tab (see Figure 41) contains information about the key installed on the mobile device.

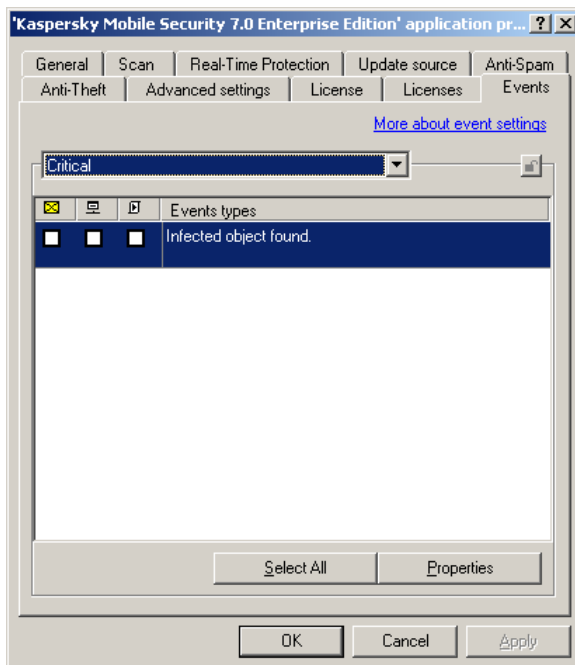
Figure 41. The **License** tab

4.9. Viewing event information

In the course of its operation Kaspersky Mobile Security generates a certain set of events. Each event has a characteristic that reflects its severity level. There are four severity levels: critical event, functional failure, warning and informational message.

Events of the same type may be of different importance level depending on the situation in which such events occurred.

The **Events** tab (see Figure 42) displays the types of events occurring in the application's operation and logged into the report as well as the location of the report and the mode of the notification of the administrator and other users that the event has occurred.

Figure 42. The **Events** tab

APPENDIX A. KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

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

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you,

via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site: <http://www.kaspersky.com/>

Virus Encyclopedia: <http://www.viruslist.com/>

Anti-virus laboratory: newvirus@kaspersky.com
(only for sending archives of suspicious objects)
<http://support.kaspersky.ru/virlab/helpdesk.html>
(for queries to virus analysts)

APPENDIX B. KASPERSKY LAB

END USER LICENSE

AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

- 1.1. **Software** means software including any Updates and related materials.
- 1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.
- 1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.
- 1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization," without limitation, includes any partnership, li-

mitted liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

- 1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.
- 1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.
- 1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

2. **Grant of License**

- 2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to “use”) the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the “License”) and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each purchased license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

- 2.2. If the Software was purchased on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package.
- 2.3. If the Software was purchased via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You purchased the License to the Software.
- 2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost,

destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using of the Software.

- 2.5. You can transfer the non-exclusive license to use the Software to other individuals or legal entities within the scope of the license granted from the Rightholder to You provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and substitute you in full in the license granted from the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software including the back-up copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User who purchased the Software from the Rightholder.
- 2.6. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was purchased on a physical medium) or specified during purchase (if the Software was purchased via the Internet):
 - Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
 - Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term

- 3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.
- 3.2. If the Software was purchased on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.

- 3.3. If the Software was purchased via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during purchase.
- 3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline.
- 3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.
- 3.6. If You have purchased the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
- 3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.
- 3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.
- 3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. Technical Support

The Technical Support described in Clause 2.6 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: <http://support.kaspersky.com>

5. Limitations

- 5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the ex-

tent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

- 5.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.5 of this Agreement.
- 5.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.5 of this Agreement.
- 5.4. You shall not rent, lease or lend the Software to any third party.
- 5.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.
- 5.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.
- 5.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

6. Limited Warranty and Disclaimer

- 6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.

- 6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.
- 6.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.
- 6.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.6 of this Agreement.
- 6.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 this Agreement or after the License to use the Software is terminated for any reason.
- 6.6. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DICLOSED TO THE RIGHTHOLDER .

7. Exclusion and Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR

FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE Rightholder OR ANY OF ITS PARTNERS, EVEN IF THE Rightholder OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE Rightholder AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE Rightholder OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

8. GNU and Other Third Party Licenses

The Software may include some software programs that are licensed (or sub-licensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

9. Intellectual Property Ownership

- 9.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners (“Trademarks”). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner’s name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.
- 9.2 You acknowledge that the source code, activation code and/or license key file for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.
- 9.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

10. Governing Law; Arbitration

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

11. Period for Bringing Actions.

No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

12. Entire Agreement; Severability; No Waiver.

This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

13. Contact Information.

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.