

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: August, 2008

Table of Contents

CHAPTER 1. MANAGEMENT VIA KASPERSKY ADMINISTRATION KIT	5
CHAPTER 2. APPLICATION DEPLOYMENT	8
2.1. Creating an installation package	8
2.2. Installing the application using a remote installation task.....	9
2.3. Installing the application using SMS	20
2.4. Adding device to a group	22
CHAPTER 3. MANAGING POLICIES	25
3.1. Creating a policy	25
3.2. Viewing and editing policy settings	32
3.2.1. Viewing application information.....	33
3.2.2. Viewing results of applying of the policy	34
3.2.3. Configuring settings of application operation event registration.....	35
3.2.4. Configuring anti-virus scan settings	36
3.2.5. Configuring Real-Time Protection operation settings.....	38
3.2.6. Selecting the application bases update source	38
3.2.7. Configuring Anti-Spam settings.....	39
3.2.8. Configuring Anti-Theft settings	41
3.2.9. Configuring additional settings	42
CHAPTER 4. MANAGING APPLICATION OPERATION SETTINGS.....	44
4.1. Viewing application information	45
4.2. Viewing information about anti-virus scan settings	46
4.3. Viewing information about Real-Time protection settings.....	47
4.4. Viewing information about update source	48
4.5. Viewing information about Anti-Spam operation settings	49
4.6. Viewing information about Anti-Theft operation settings.....	50
4.7. Viewing information about additional settings	51
4.8. Viewing key details	52
4.9. Viewing event information	53
APPENDIX A. KASPERSKY LAB.....	55
A.1. Other Kaspersky Lab Products	56

A.2. Contact Us.....	66
APPENDIX B. LICENSE AGREEMENT.....	67

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.

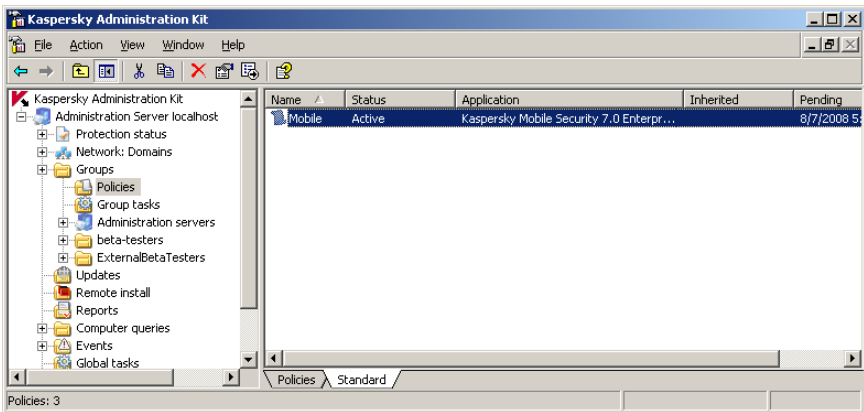


Figure 1. Kaspersky Administration Kit Administration Console

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.

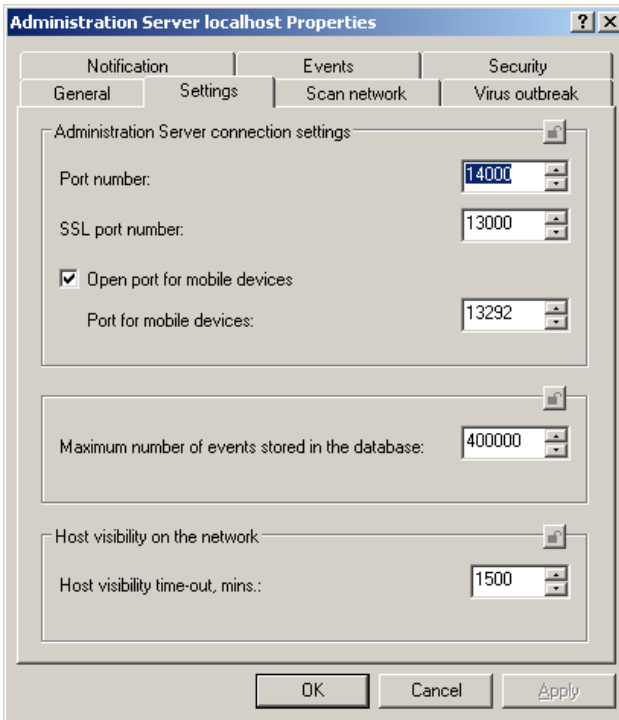


Figure 2. The **Settings** tab

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)

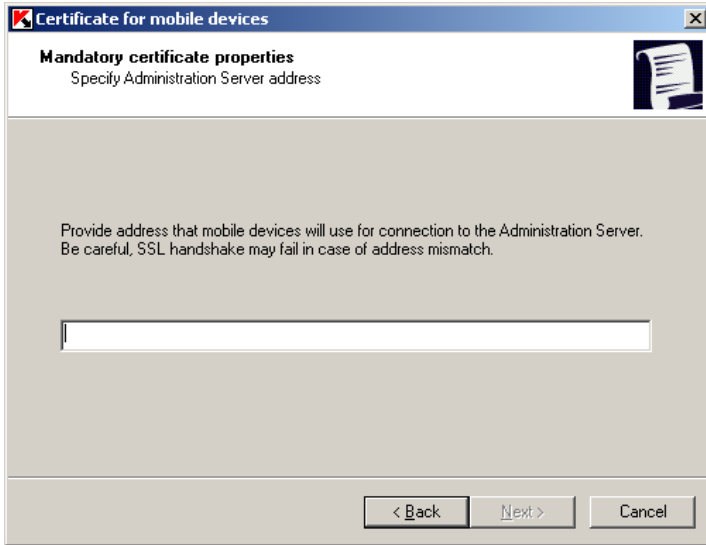


Figure 3. Creating a certificate for mobile devices

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 installation** 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.

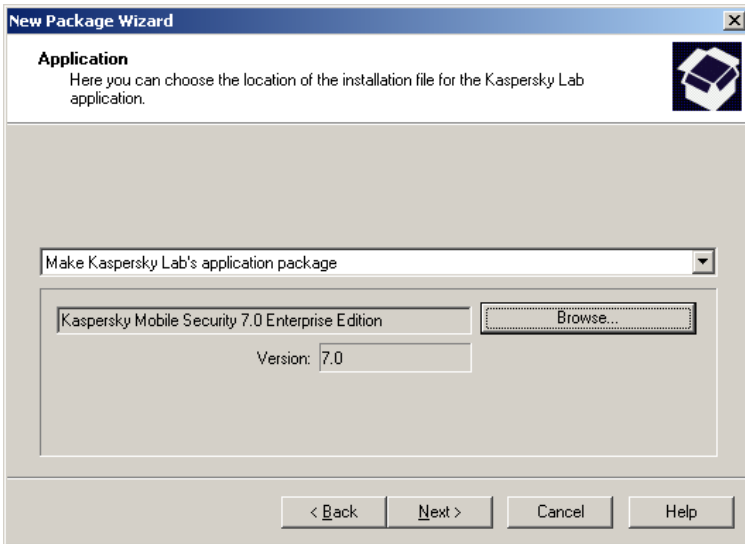


Figure 4. Creating an installation package Selecting application to be installed

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** mode 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 on 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.

4. When selecting the application and determining the task type (see Figure 5) set values **Kaspersky Administration Kit** and **Remote application installation** respectively.
5. 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.

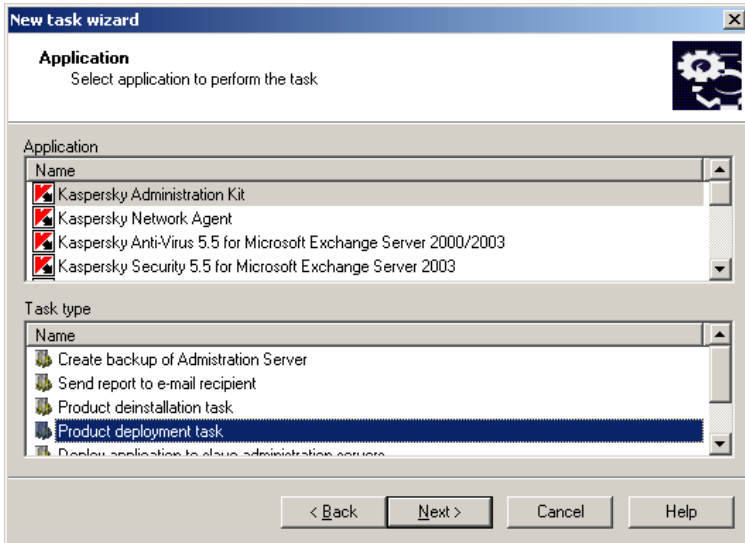


Figure 5. Determining the task type

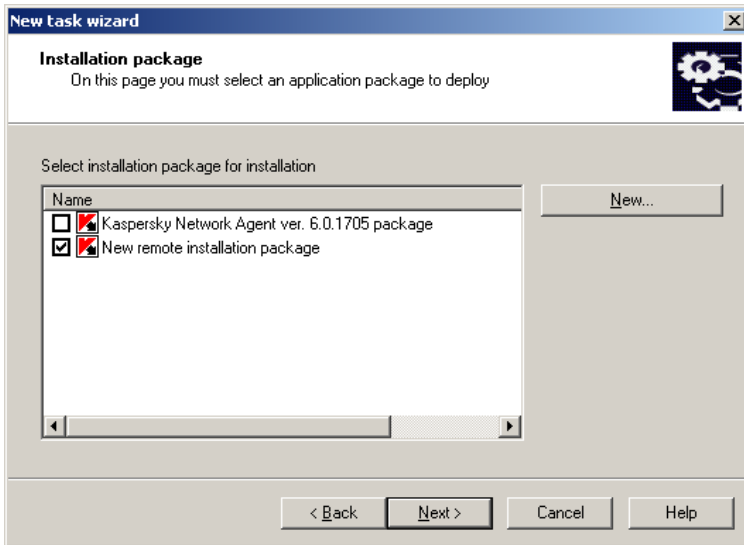


Figure 6. Selecting an installation package to be installed

- At this stage select the **Forced installation** option (see Figure 7).

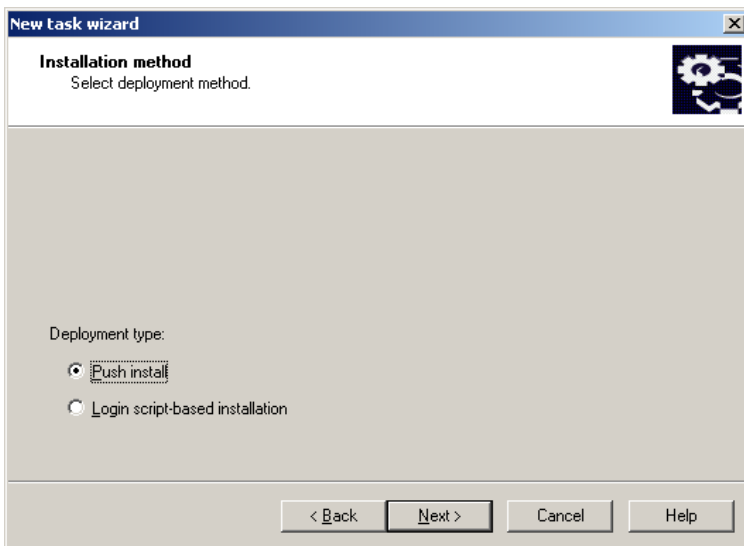


Figure 7. Determining the installation type

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 **Downloading installation package** group of fields:

- Check the **With Windows tools from the public access 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 (check 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 the Administration 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 **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.

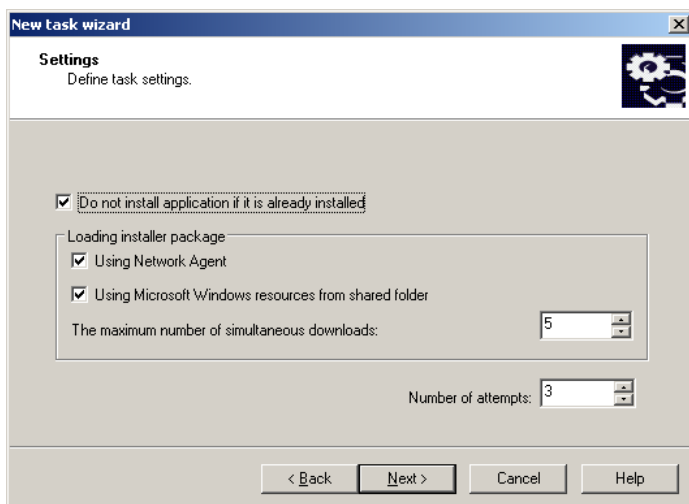


Figure 8. Additional installation options

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 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 **New** button.

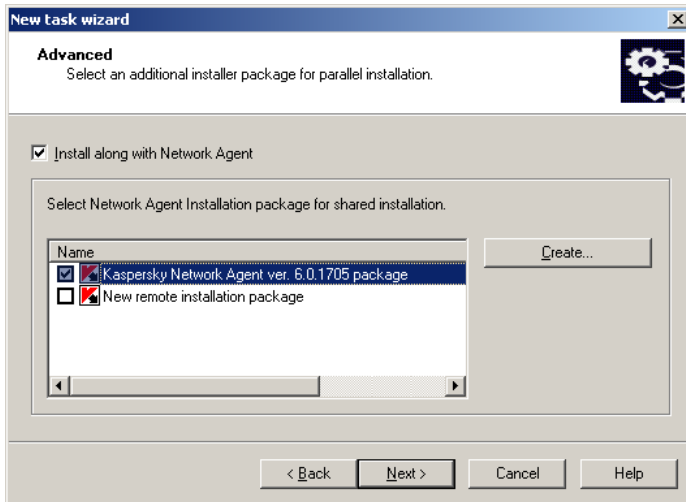


Figure 9. Selecting joint installation with the Network Agent

9. Determine the method to select computers for which the task will be created (see Figure 10):
 - **Based on the data obtained by polling the Windows network.** In this case computers for installation will be selected based on the data obtained by the Administration server by polling the corporate Windows network.
 - **Based on addresses (IP address, NetBIOS name or DNS name), entered 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 **Group** folder) or computers that are not yet included into its structure (the **Network** folder).

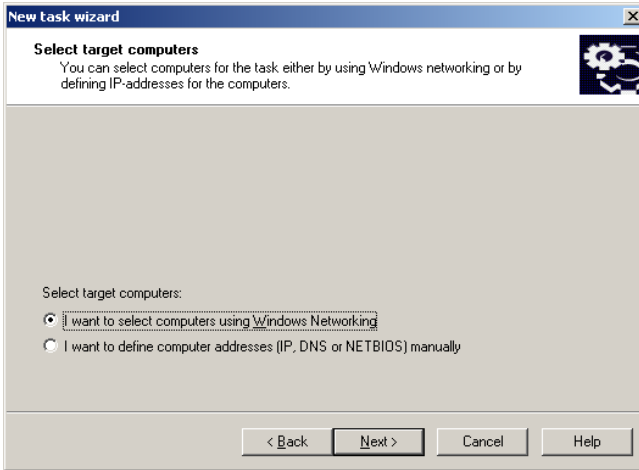


Figure 10. Determining the methods to select client computers

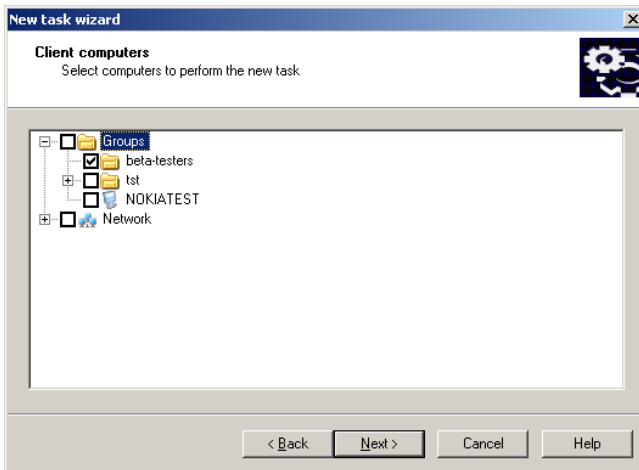


Figure 11. Creating a list of computers for installation based on Windows network data

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).

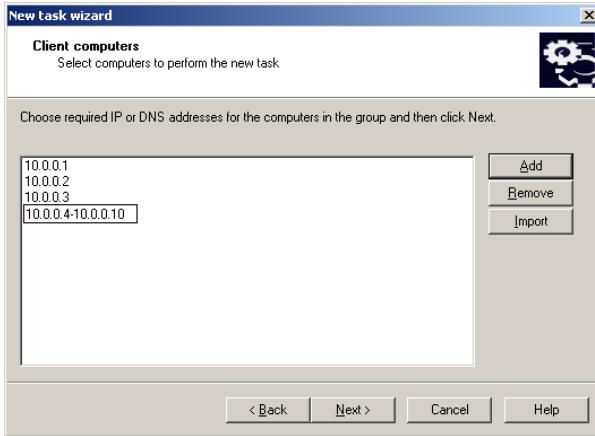


Figure 12. Creating a list of computers for installation based on IP addresses

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

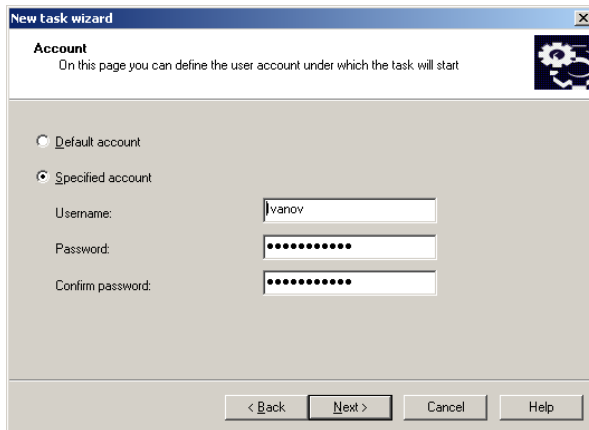


Figure 13. Selecting an account

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.
- **Specify the 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 launch** drop-down list:
 - **Manually.**
 - **Every N hour(s).**
 - **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).
 - **Upon completion of 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).

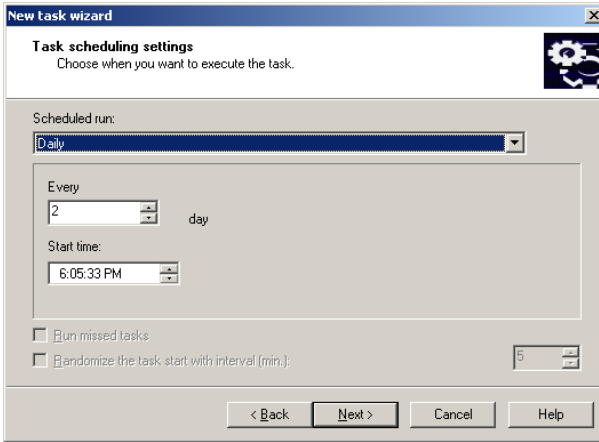


Figure 14. Daily task launch

Upon the completion of the wizard the remote installation task created will be added to the **Global task** 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.

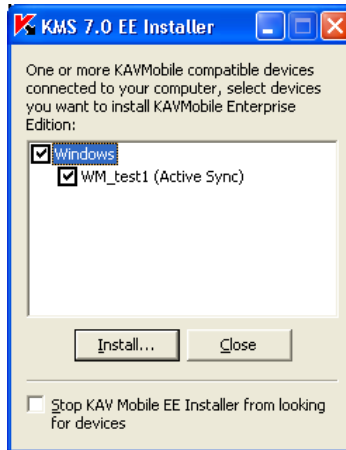


Figure 15. *KMListen.exe* utility window

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 Installation** 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 **Install using SMS** 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 **Load from file**.

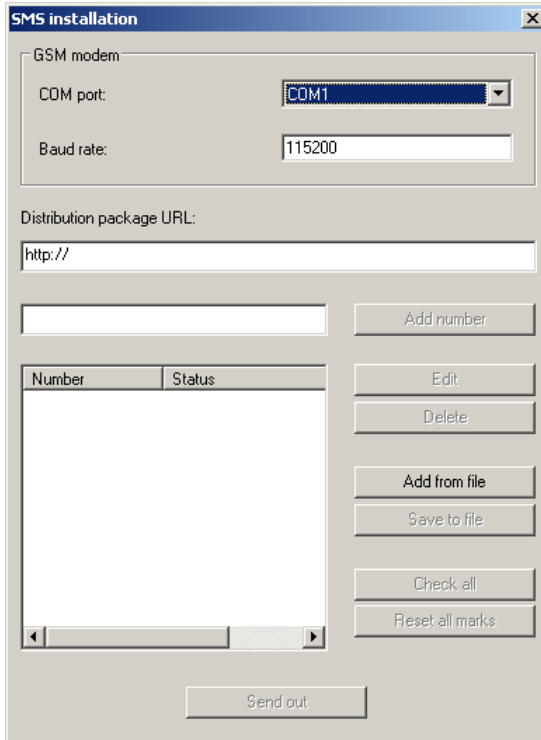


Figure 16. SMS sending settings

6. Press the **Send** 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).

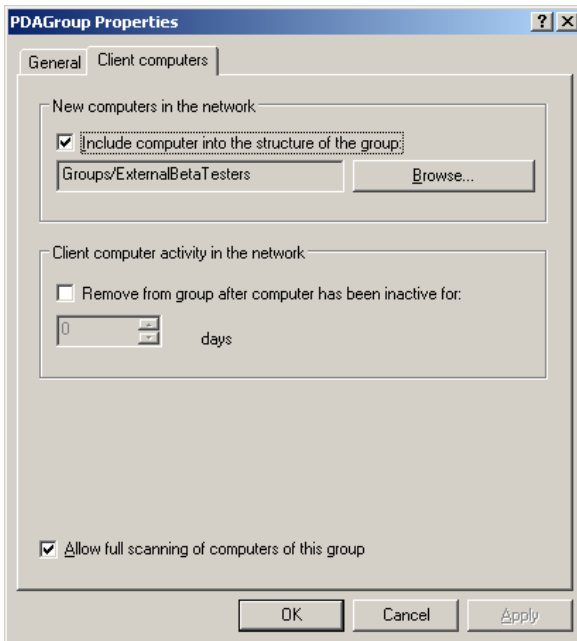


Figure 17. Group properties

4. Check the **Add computer to the group** box in the **New computer 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 only executable files** - scan executable program files only.
- **Scan archives** - scan files packed into archives.
- **Attempt to disinfect infected objects** – attempt to disinfect infected objects encountered. Not every object can be disinfected.

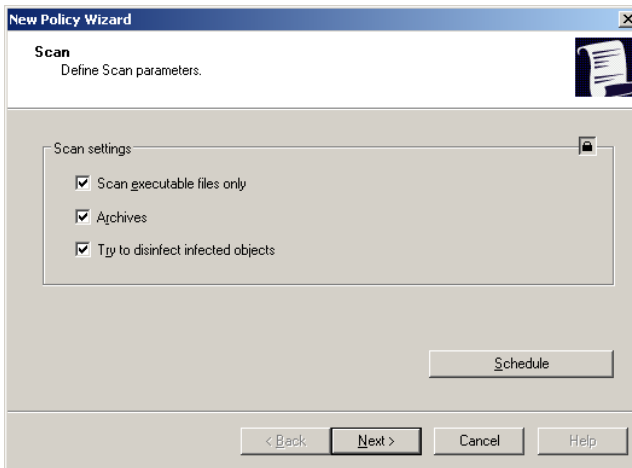


Figure 18. Configuring the anti-virus protection settings

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:

- **Manual** – 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 **Launch time** group of fields.

- **Weekly** – the action will be performed on a certain weekday. In the **Launch 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 only executable files** - scan executable program files only.

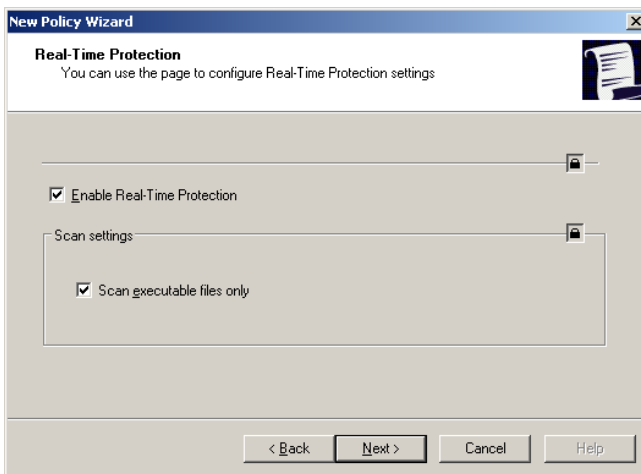


Figure 19. Configuring Real-Time Protection settings

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 Address** 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.

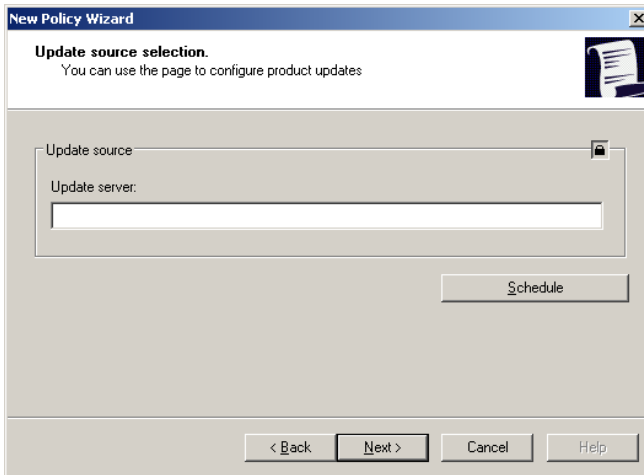


Figure 20. Selecting an update source

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 scan frequency:

- **Manual** – 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 **Launch time** group of fields.
- **Weekly** – the action will be performed on a certain weekday. In the **Launch 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 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** section:

- **Disabled.** Anti-Spam is disabled.
- **Only messages from the white list will be delivered.** In this mode Anti-Spam passes messages matching the “white list” criteria. All other messages will be blocked.
- **Only messages from the white list will be delivered.** 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.

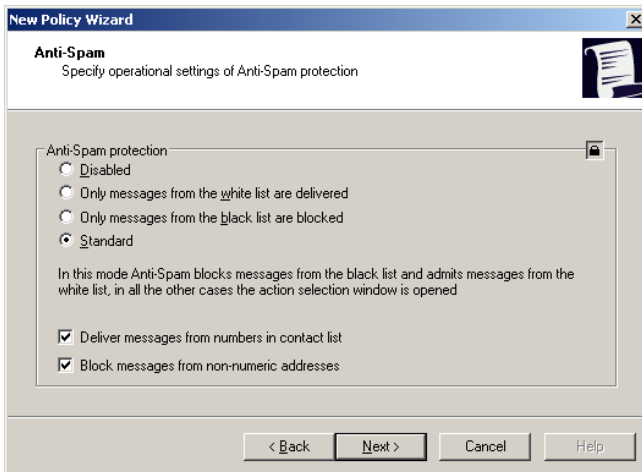


Figure 21. Configuring Anti-Spam settings

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

Check the **Block messages from non-numeric numbers** 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.** Firewall blocks all incoming connections; any outgoing connections are allowed.
- **Medium.** Firewall blocks all incoming connections; outgoing connections are allowed using ports HTTP/HTTPS/SMTP/IMAP/SSH.
- **High.** Firewall blocks any network activities except connections with the Administration Server and updates of the application bases.

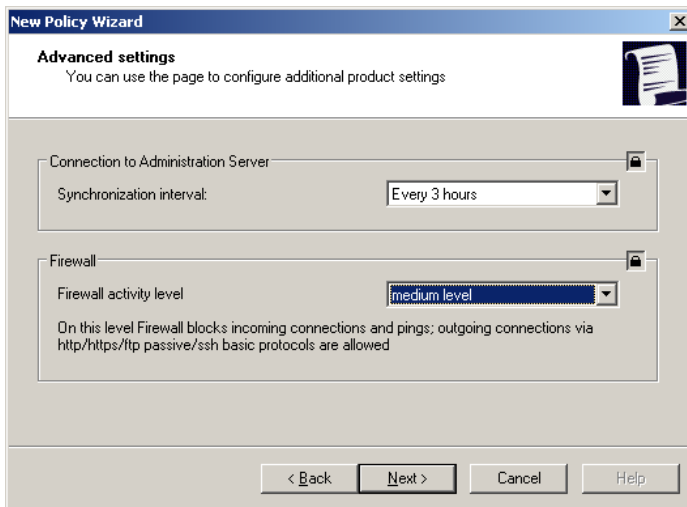


Figure 22. Additional application settings

Specify the synchronization frequency by selecting the required value from the **Synchronization Period** drop-down list in the **Synchronization with the 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.

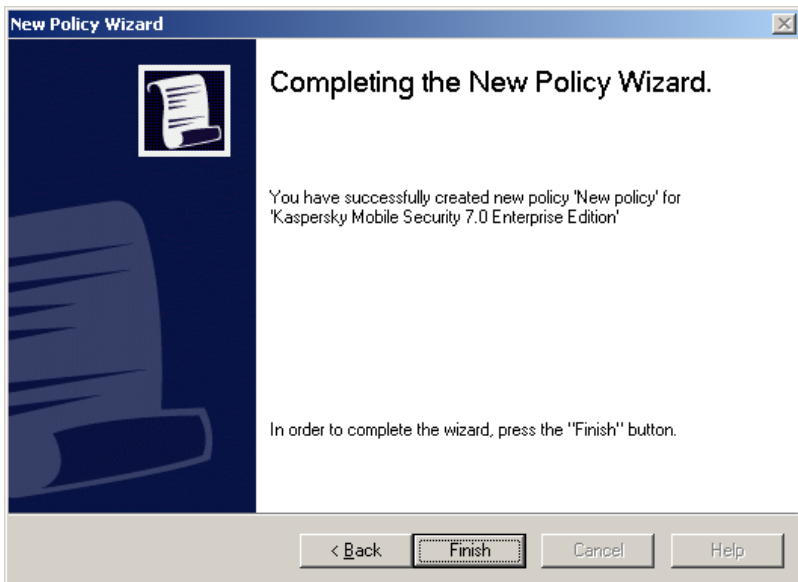


Figure 23. Completing creation of the policy

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 **Policy** 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**, **Use** 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.

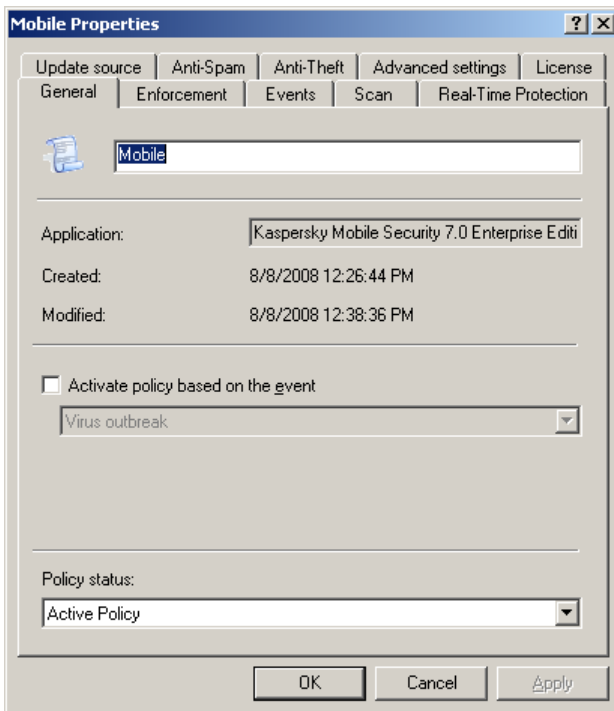


Figure 24. The **General** tab

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 **Use** 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.

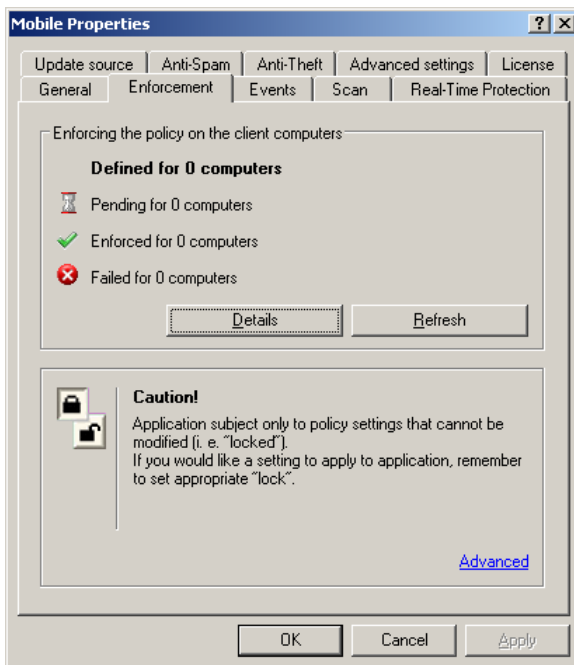


Figure 25. The **Use** tab

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.

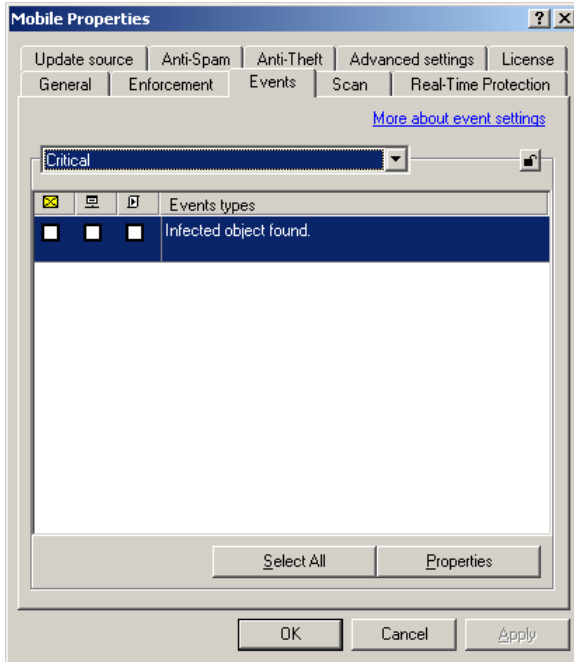


Figure 26. The **Events** tab

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.

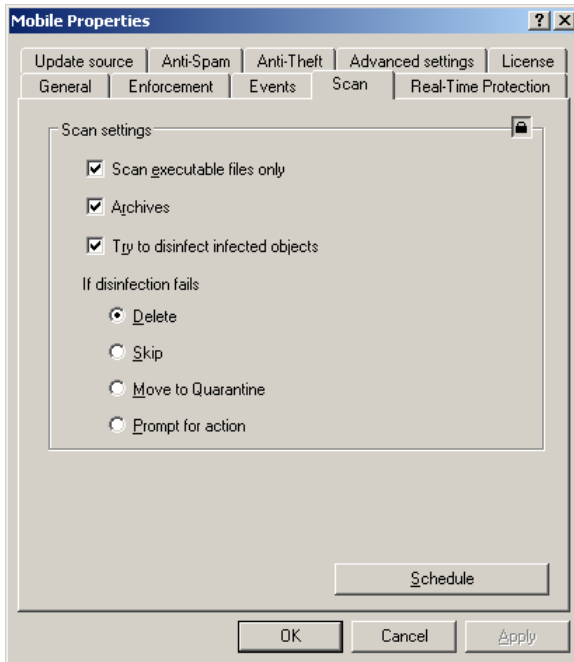


Figure 27. The **Scan** tab

Specify the action to be performed once an infected object is detected in the **Actions to be performed with infected objects** section.

- **Delete.**
- **Skip** - leave infected objects detected intact.
- **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 **Attempt to disinfect infected object** 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 25.

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.

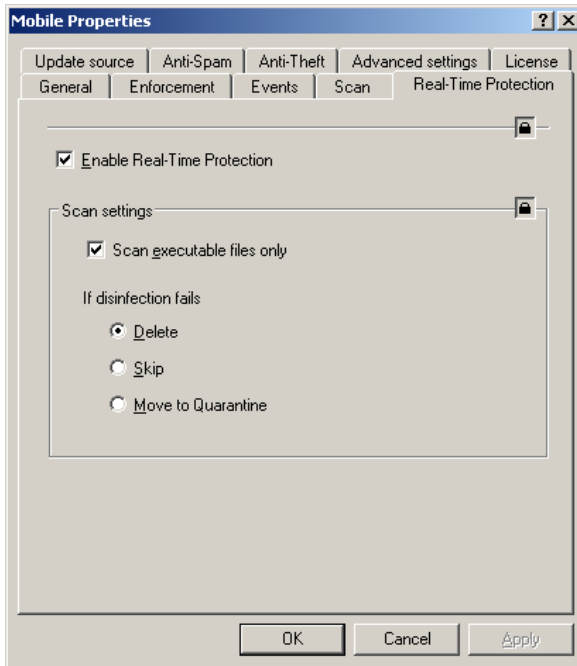


Figure 28. The **Real-Time Protection** tab

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 Address** 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.

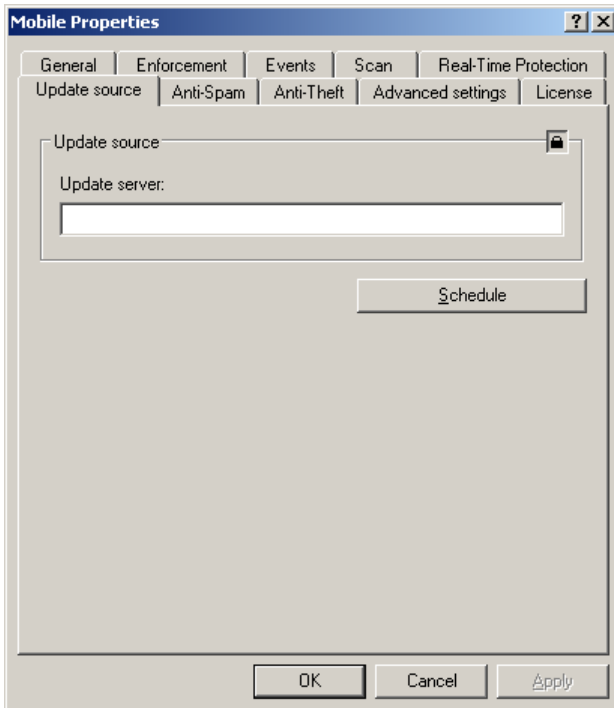


Figure 29. The **Update source** tab

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.

- **Deliver only message from white list** – 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.
- **Block only message from black list** – 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 found in the contact list** to ensure that Anti-Spam passes messages from numbers from the contact lists.

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

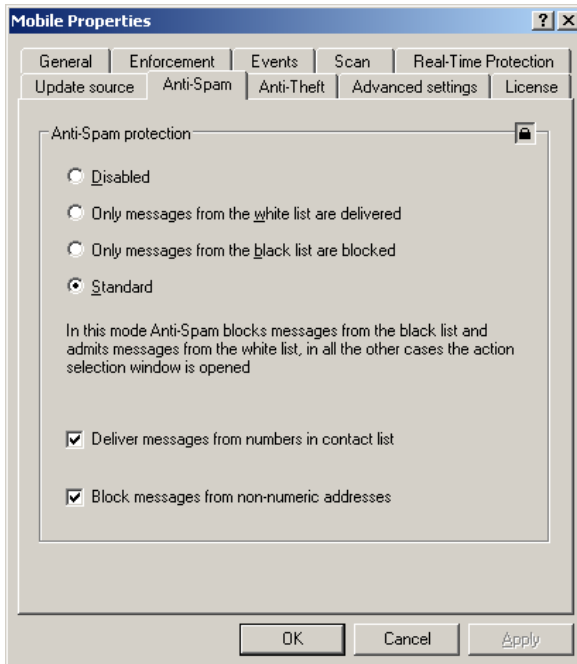


Figure 30. The **Anti-Spam** tab

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 **SMS-Clean** 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:password" 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 mail** – deletion of messages.
- **Delete documents** – deletion of personal data.
- **Delete cards from the flash card** - deletion of files from the memory card.
- **Delete network settings and access point settings** – deletion of personal network settings.

Check the **SMS-Block** 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:password» to the device.

Check the **SMS-Watch** 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 number** and **Additional number** 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.

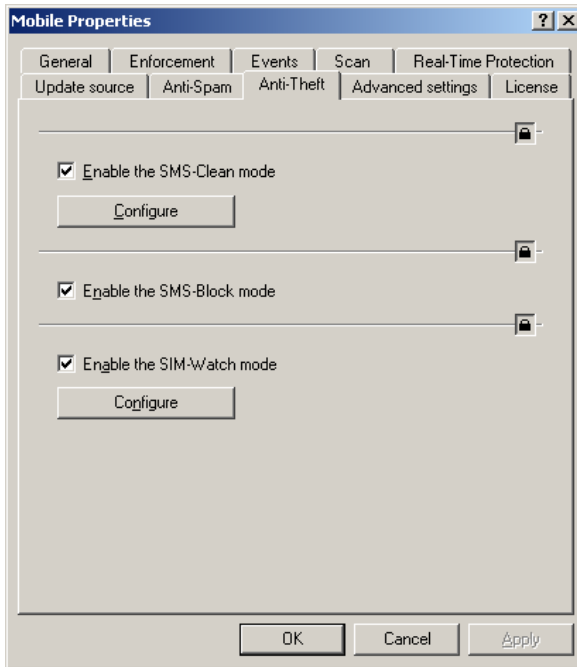


Figure 31. The **Anti-Theft** tab

3.2.9. Configuring additional settings

The **Additional 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 Period** drop-down list in the **Synchronization with the Administration Server** block.

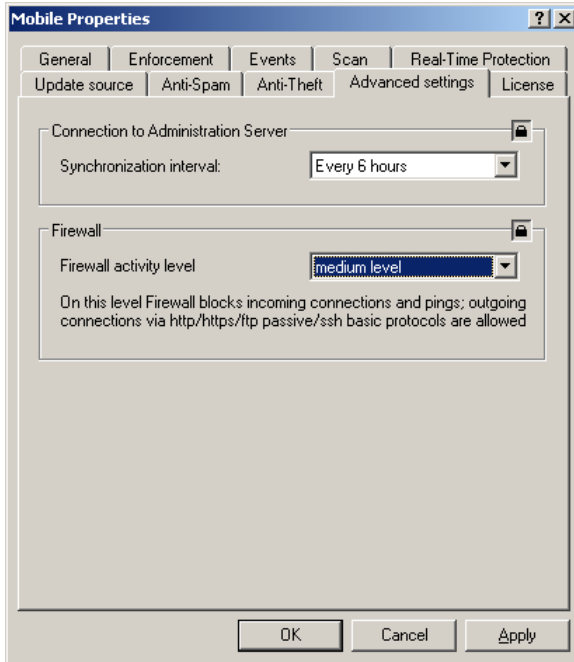


Figure 32. **Additional Settings**

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

- **Disabled** – disables the Firewall operation.
- **Low** - Firewall blocks all incoming connections; any outgoing connections are allowed.
- **Medium** - Firewall blocks all incoming connections; outgoing connections are allowed using ports HTTP/HTTPS/SMTP/IMAP/SSH.
- **Highest** - 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 25).

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 **Actions** 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).

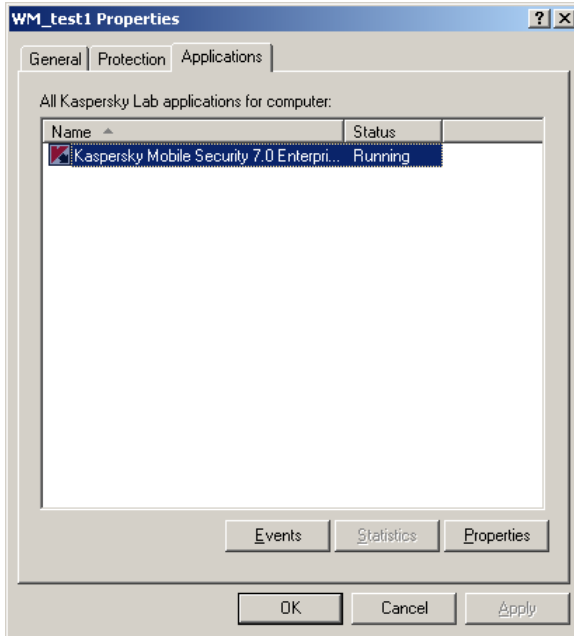


Figure 33. Mobile device properties viewing window.
The **Applications** tab

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 settings.

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.

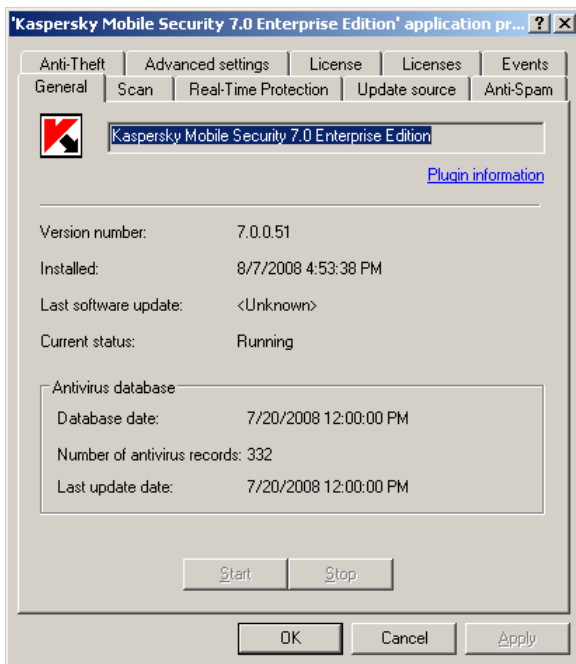
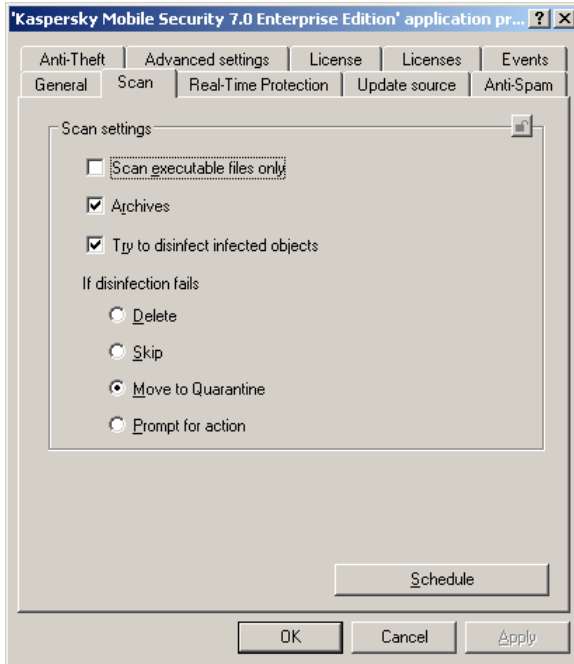


Figure 34. Application settings configuration window.
The **General** tab

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 about 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.

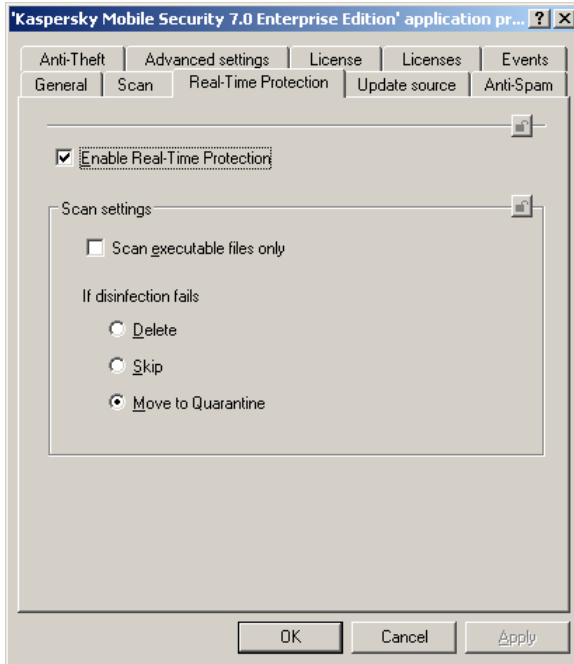


Figure 36. The **Real-Time protection** tab

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.

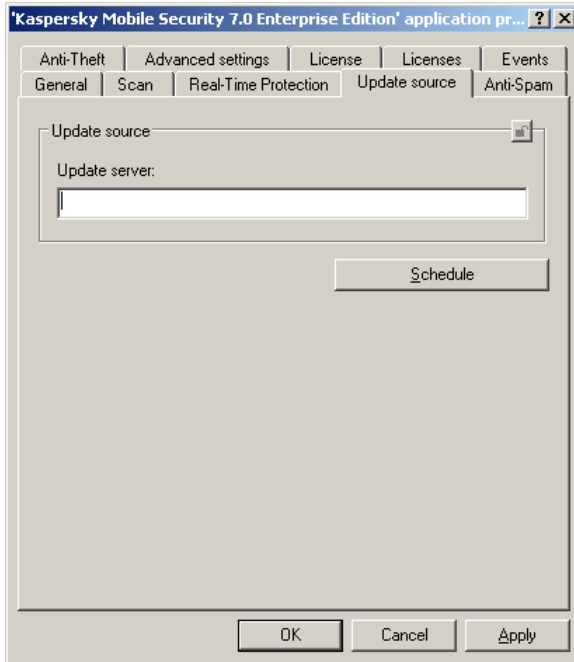


Figure 37. The **Update Source** tab

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.

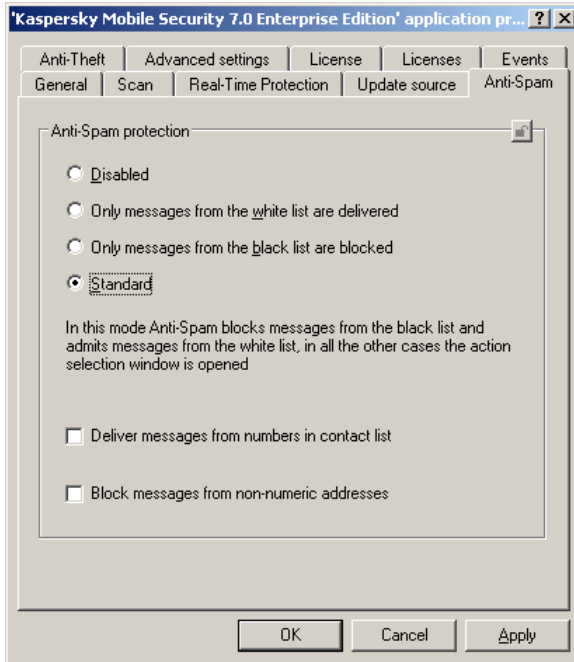
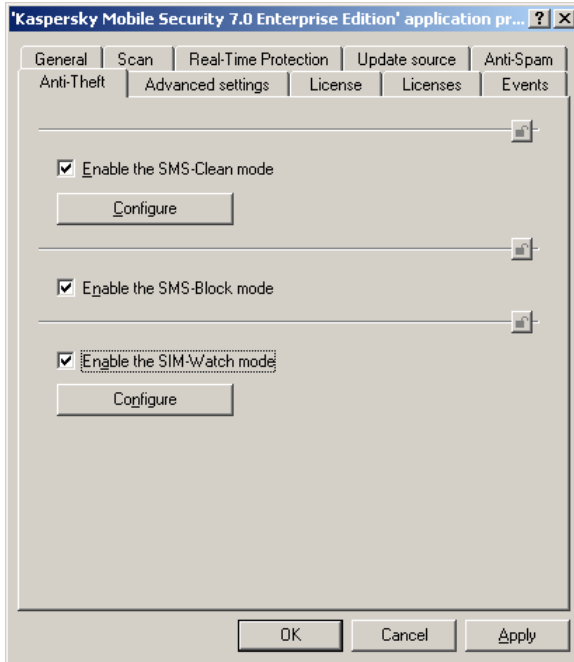


Figure 38. The **Anti-Spam** tab

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 section.

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

4.7. Viewing information about additional settings

Using the **Additional 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.

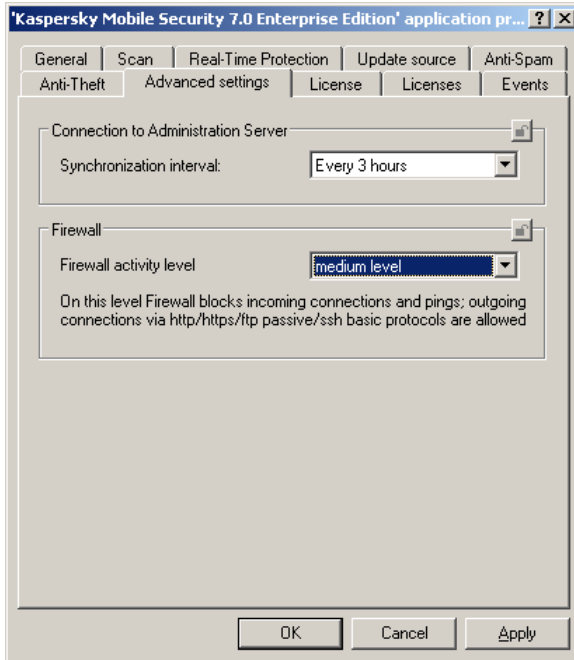
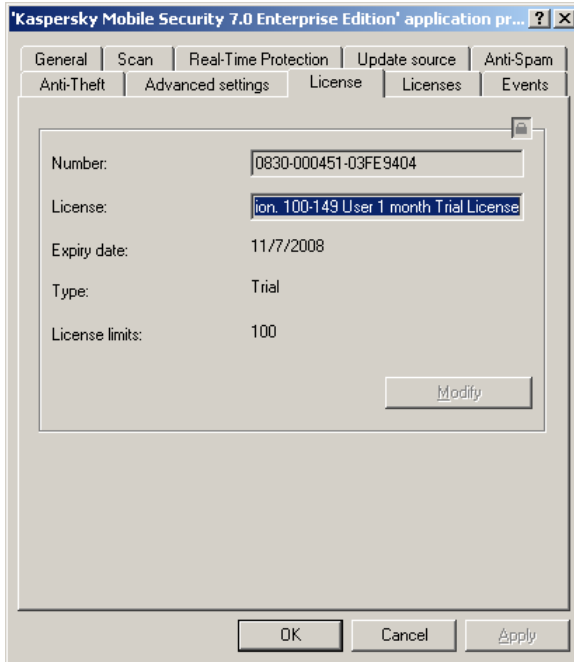


Figure 40. The **Additional Settings** tab

4.8. Viewing key details

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

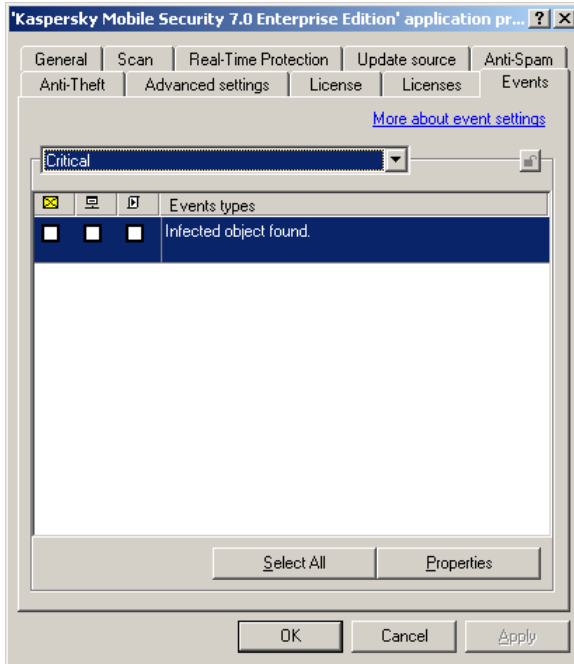
Figure 41. The **License** tab

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

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 Internet Security, 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 Internet Security 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.

A.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 taskbar notification area
- 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.

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.

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 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 Network.
- 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.

A.2. Contact Us

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

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

APPENDIX B. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY MOBILE SECURITY ENTERPRISE EDITION (“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/DVD’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/DVD’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.

All references to “Software” herein shall be deemed to include the software activation code with which you will be provided by Kaspersky Lab as part of the Kaspersky Mobile Security 7.0 Enterprise Edition.

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. You may install one copy of the Software on one device.

1.1 *Use.* The Software is licensed as a single product; it may not be used on more than one device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is “in use” on a device 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/DVD-ROM, or other storage device) of that device. 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 device against viruses and network attacks whose signatures are contained in the threat signatures and network attacks databases which are available on Kaspersky Lab's update servers.

1.1.3 If you sell the device 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 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 provide the activation code or license key file to third parties or allow third parties access to the activation code or license key. The activation code and license key are confidential 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 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.

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 activation on:

- (a) payment of its then current support charge, and;
- (b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to enter activation code which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

Support Services shall become available after Software activation. Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

(ii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iv) "Support Services" means:

- (a) Hourly updates of the anti-virus database;
- (b) Updates of network attacks database;

- (c) Updates of anti-spam database;
 - (d) Free software updates, including version upgrades;
 - (e) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
 - (f) Virus detection and disinfection updates in 24-hours period.
- (v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your device.

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 and spam letters, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) 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.

- (v) 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.
- (vi) 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).