

KASPERSKY LAB

---

Kaspersky Anti-Virus<sup>®</sup>  
Mobile 6.0 Enterprise Edition

User's Guide

KASPERSKY ANTI-VIRUS® MOBILE 6.0  
ENTERPRISE EDITION

---

# User's Guide

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

Revision date: October 2007

# Contents

CHAPTER 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION .....	4
1.1. Hardware and software requirements .....	5
1.2. Product package.....	5
CHAPTER 2. KASPERSKY ANTI-VIRUS FOR MICROSOFT WINDOWS MOBILE .....	6
2.1. Installing Kaspersky Anti-Virus.....	6
2.2. Using the application .....	9
2.2.1. Starting the application .....	9
2.2.2. Graphical user interface .....	10
2.2.3. Anti-virus scan and protection .....	11
2.2.4. Using the Quarantine.....	15
2.2.5. Using Anti-Spam.....	16
2.2.6. Updating the anti-virus bases.....	19
2.2.7. Receiving reports about the application's operation .....	20
2.3. Removing the program.....	21
CHAPTER 3. MANAGING THE APPLICATION USING KASPERSKY ADMINISTRATION KIT.....	24
3.1. Managing policies.....	25
3.1.1. Creating a policy .....	26
3.1.2. Viewing and editing policy settings .....	30
3.2. Managing application settings.....	37
APPENDIX A. KASPERSKY LAB.....	45
A.1. Other Kaspersky Lab Products .....	46
A.2. Contact Us.....	56
APPENDIX B. LICENSE AGREEMENT .....	57

---

# CHAPTER 1. KASPERSKY ANTI-VIRUS MOBILE 6.0 ENTERPRISE EDITION

Kaspersky Anti-Virus® Mobile Enterprise Edition (hereafter also referred to as **Kaspersky Anti-Virus**) is designed to protect mobile devices running Microsoft Windows Mobile against malicious programs and unwanted messages and provides the following features:

- **Real-time protection** of the device's file system – interception and scan of:
  - all incoming objects, transferred by means of wireless connections (infra-red port, Bluetooth), EMS and MMS messages, during synchronization with a personal computer and loading files through a browser;
  - files, opened on the mobile device;
  - programs, installed using the device's interface.
- **On-demand or scheduled scans** of file system objects stored either on your mobile device or on memory extension cards.
- **Secure isolation of infected objects** in Quarantine.
- **Updating of Kaspersky Anti-Virus bases** used to detect malicious applications and delete unsafe objects.
- **Blocking of unwanted SMS messages.**

Kaspersky Anti-Virus can only be installed with the help of Kaspersky Administration Kit tools which also allows the administrator to perform the following actions with Kaspersky Anti-Virus:

- receive information about the protection status;
- receive information about the current application parameters;
- modify settings of the application parameters using policies;
- receive information about meaningful events.

Unlike other Kaspersky Lab's products, Kaspersky Anti-Virus **does not allow** performing the following actions using Kaspersky Administration Kit tools:

- download anti-virus base updates;
- create group / global / local tasks;
- extend the license key validity period;
- remotely uninstall the application.

The application has an easy-to-use menu and a user-friendly interface allowing the user to control Kaspersky Anti-Virus settings (modification of which is not prohibited by the policy), to view the current status of the anti-virus protection and the event log registering the program's actions.

Upon detection of a malicious application, Kaspersky Anti-Virus can disinfect the infected object (if disinfected is possible), delete it or move it to Quarantine. No copies of an object being deleted will be saved.

## **1.1. Hardware and software requirements**

Kaspersky Anti-Virus can be installed on mobile devices running one of the following operating systems:

- Microsoft Windows Mobile 2003, 2003SE.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

## **1.2. Product package**

Kaspersky Anti-Virus Mobile Enterprise Edition can be purchased via the Internet, enabling the download of the installation program and electronic documentation. You can also purchase Kaspersky Anti-Virus Mobile Enterprise Edition at mobile service offices. For purchase details, please contact your mobile operator.

---

# CHAPTER 2. KASPERSKY ANTI-VIRUS FOR MICROSOFT WINDOWS MOBILE

This chapter contains description of the operation of Kaspersky Anti-Virus Mobile Enterprise Edition for mobile devices running one of the following operating systems:

- Microsoft Windows Mobile 2003, 2003SE,
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

## 2.1. Installing Kaspersky Anti-Virus

Installation of Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition is performed remotely using Kaspersky Administration Kit.

- Creation of the installation package that includes the product's distribution file, installation utility, license key, configuration file.
- Copying of the installation package to the remote computer; at this time the installation utility will be launched on the computer; the utility will be waiting for the mobile device to be connected to the computer.
- Installation of Kaspersky Anti-Virus on the mobile device when the device is connected to the computer.

*In order to install Kaspersky Anti-Virus Mobile Enterprise Edition, perform the following steps:*

1. In the **Remote Install** folder of the console tree create an installation package that will be used for remote installation of the application onto the mobile devices (see Figure 1).

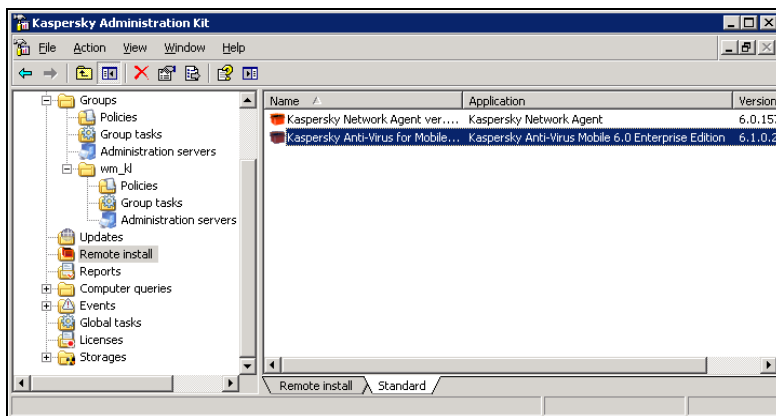


Figure 1. Selecting the installation package

For more details about creating and using installation packages see Kaspersky Administration Kit Reference Guide.

2. Open the shortcut menu for the selected package and use the **Install** command.

Installation of the installation package is implemented as a Microsoft Windows wizard and includes a sequence of dialog boxes (steps) navigated using the **Back** and **Next** and completed using the **Finish** button. To exit the wizard at any step, use the **Cancel** button.

**Attention!**

The installation package includes the license key which must be installed to a mobile device together with the package itself. If there is no license key in the installation package, the application will not be considered activated and will not work.

License key installation by any other method is not supported!

3. As a result of the actions performed by the wizard, utility **Kav Mobile EE Installer** will be installed on the selected computer or a group of computers; this utility will be used to perform further installation of Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.
4. When connecting a mobile device to the computer, Kav Mobile EE Installer will suggest that the user installs Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition on this device (see Figure 2).

**Attention!**

In order to install Kaspersky Anti-Virus 6.0 Enterprise Edition on a

mobile device Microsoft Active Sync must be used, otherwise the **Kav Mobile EE Installer** will not be able to detected the connected devices.

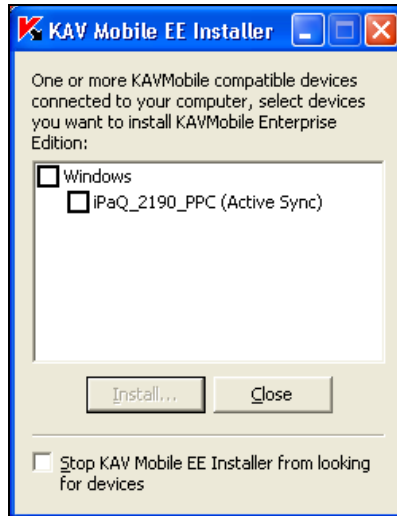


Figure 2. Selecting a mobile device

5. Select a device from the list of suggested devices and press the **Install** button. Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition installation process on the selected mobile device will then be started.
6. Read the text of the licence agreement on the mobile device. If you agree to all the terms, press **OK**. To abort the installation, press **Cancel** (see Figure 3)<sup>1</sup>.

---

<sup>1</sup> All screenshots in this document are made for I-mate K-JAM smartphone. For other models of smartphones, the application interface may slightly differ.




Figure 3. Licence Agreement

## 2.2. Using the application

This section contains information about configuration of the settings of the anti-virus and real-time protection, SMS messages filtering, mobile device anti-virus scan and the application updates.

### 2.2.1. Starting the application


*To launch Kaspersky Anti-Virus Mobile Enterprise Edition, perform the following:*

1. Open the **Applications** menu on your mobile device.
2. Select the  **KAV Mobile** icon and start the application.

After the applications startup the mobile device will display a window containing the status of the main components of Kaspersky Anti-Virus (see Figure 4).

- **Protection** - using the real-time protection mode. For more details see section 2.2.3 on page 11).
- **Last Full Scan** – date of the last anti-virus smartphone scan.
- **Database Release Date** – date of release of Kaspersky Anti-Virus bases used by the application.

**Attention!**

Attention! If the Anti-Virus scan of a mobile has not been performed or two weeks have passed since the moment the anti-virus bases had been updated last time, the icon next to the corresponding item will change to . Such icon also appears if the mode of real-time protection or the Anti-Spam module is disabled.

- **Anti-spam** – Anti-spam operating mode used for filtering SMS messages.

**Attention!**

The Anti-spam component is unavailable on PDA!

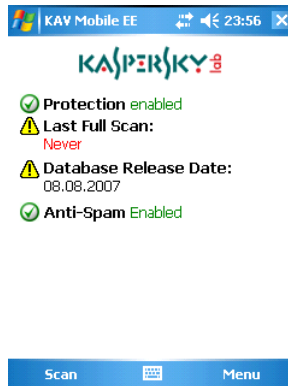


Figure 4 Application components status window

## 2.2.2. Graphical user interface

The graphical user interface (GUI) contains five tabs that you can access using the **Menu** (see Figure 6):

- Using the **Scan menu** tab you can perform an anti-virus scan of the mobile device, edit the anti-virus scan and real-time protection mode settings and configure the auto scan schedule.
- Using the **Anti-Spam menu** tab you can configure filtering of incoming SMS and MMS messages.
- Using the **Updater menu** tab you can update the anti-virus bases, edit the updating settings and configure the updating schedule.

- Using the **Quarantine** tab you can manage the quarantine – a special-purpose storage for infected and suspicious objects.
- Using the **Information** tab you can view the logs of the operation of the application's components, general information about the application and about the bases used and edit the general settings of the application's operation.

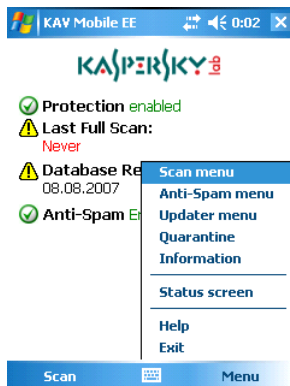


Figure 6. The application Menu

In order to return to the application components status window, select the **Status Screen** item.

In order to close the application select **Exit**.

## 2.2.3. Anti-virus scan and protection

Using the **Scan** tab, you can perform an anti-virus scan of the entire file system and memory of the mobile device or a scan of an individual file or directory. You can also modify the anti-virus scan settings and the anti-virus protection mode, view a report about the scan results or configure a schedule of an automatic scan launch.

### 2.2.3.1. Real-time protection and on-demand scan

Real-time protection is an operating mode in which the resident part of Kaspersky Anti-Virus is permanently loaded in the RAM of the mobile device and monitors all data in the device.

The real-time protection starts at the moment when the device is turned on and runs until the device is off (if the use of the mode is not disabled in the settings).

Additionally Kaspersky Anti-Virus allows performing full scan of the mobile devices' file system.

Information about the results of the real-time protection and on-demand scan is entered into a report. In order to view the report, select the **Scan report** item. The report can also be accessed via the **Information** tab (see section 2.2.7 on page 20).

*In order to enable the real-time protection mode perform the following:*

1. Select the **Scanner settings** item on the **Scan menu** tab.
2. Enable/disable the real-time protection mode by setting the corresponding value of the **On-Access Scan** setting.

*In order to modify the on-demand scan settings, do the following:*

1. Select the **Scanner settings** item on the **Scan menu** tab.
2. Specify the scan area in the **Scan options** block by selecting types of files to be scanned as follows:
  - **Scan archives** - scan files packed in archives;
  - **Executables only** - scan only executable files.
3. In block **If a virus is detected** specify the action to be performed by the application upon detection of an infected object. To make Kaspersky Anti-Virus attempt to disinfect the infected object detected check the **Try to disinfect** box. If no disinfection is required, select a possible Anti-Virus action by specifying one of the following values for the **If disinfection failed** setting:
  - **Quarantine** – move infected objects detected to quarantine
  - **Ask User** – display a message about the virus detection on the screen with a suggestion to either delete the infected object, quarantine or skip it.
  - **Delete** – delete infected objects detected
  - **Report only** – do not perform any action with the infected objects

You can also specify one of these actions for a case when an attempt to disinfect an infected object may be unsuccessful. In order to do it check the **Try to disinfect** box and select the action you need in the **If disinfection failed** list.

*In order to start an anti-virus scan:*

1. Start Kaspersky Anti-Virus (see section 2.2.1 on page 9).

2. Switch to the **Scanner settings** tab.
  - Specify the scan scope in the **Scan options** block by selecting the file types to be scanned (see above).
  - Determine the actions to be performed by the application once an infected object is detected (see above).
3. Select the **Scan phone** time on the **Scan menu** tab (see Figure 7) if you wish to scan the entire file system of the mobile device or **Scan folder** if you wish to scan an individual folder.

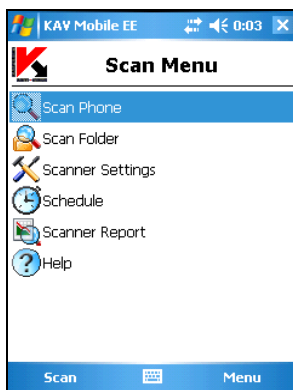


Figure 7. The **Scan menu** tab

When the **Scan folder** item is selected, you will switch to the window that displays the mobile device's file system. In order to start a folder scan, move the cursor to the folder to be scanned and press the **Scan** button.

After the scan is started, a scan window will open that displays the current status, the number of objects scanned and the path to the object being currently scanned (see Figure 8).

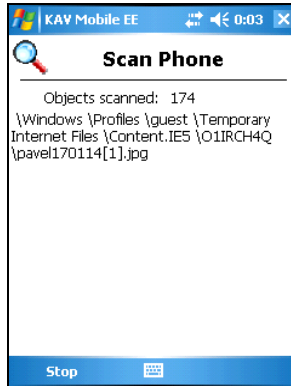
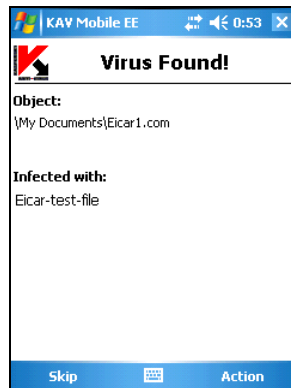
Figure 8. The **scan** window

Figure 9. Notification of a virus detection

After the scan is completed, the application will display the general statistics about detected and deleted malicious objects.

### 2.2.3.2. Scheduled scan

With Kaspersky Anti-Virus, you can schedule automatic mobile device scans to start at specified time. Scanning will be running in background mode. Upon a detection of an infected object, the application performs the action specified in its scan settings (see section **Scanner settings**).

Scheduled scanning is disabled by default.

To configure a scheduled scan, perform the following steps:

Use the **Scan menu** page to select the **Schedule** item and configure the scan parameters (see Figure 10):

- **Daily** – the scan will be performed every day. The scan time is determined by the **Time** parameter.
- **Weekly** – the scan will be performed every week. The scan day and time are determined by the **Day of week** and **Time** parameters.
- **Manual** - the scan will only be started manually by the user.

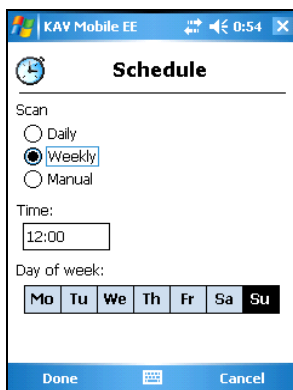


Figure 10. The **Schedule** menu

## 2.2.4. Using the Quarantine

Quarantined infected objects are unable to harm your mobile device and you can later delete or restore them later.

The application can relocate detected infected objects to the Quarantine automatically or after your confirmation.

If you wish to configure the application to quarantine infected objects automatically, switch to the **Scan menu** tab, select the **Scanner settings** and select **Quarantine** as the value of the **If disinfection failed** setting in the **If a virus is detected** block. If disinfection of the infected object was unsuccessful, check the **Try to disinfect** box and select **Quarantine** in the **If disinfection failed** list.

If you have selected **Ask User** as the action to be performed, then upon detection of an infected object Kaspersky Anti-Virus will offer you to delete or quarantine it.

You can use the **Quarantine** page to view the Quarantine content (see Figure 12).



Figure 12. **Quarantine**

The menu accessible in the Quarantine window allows you to:

- View detailed information about any object stored in Quarantine (**Detailed info**).
- Scan a quarantined file for viruses (**Scan**).
- Delete the current object (**Delete file**).
- Disinfect a quarantined object (**Disinfect**).
- Restore the current object from Quarantine to its original folder (**Restore**).
- Purge Quarantine removing all objects stored in it (**Empty quarantine**).

## 2.2.5. Using Anti-Spam

Anti-Spam is another new feature introduced in Kaspersky Anti-Virus Mobile 6.0. It is intended for mobile device protection against unwanted SMS messages.

### **Attention!**

**On PDA Anti-spam component is unavailable!**

The employed principle of message filtering is based on the so-called black and white lists. Anti-Spam will block incoming messages from phone numbers added to your black list. Messages from numbers added to the white lists will not be blocked.

In order to change the Anti-Spam settings:

1. Select **Settings** on the **Anti-Spam** menu tab.
2. Enable/disable the use of Anti-Spam by checking or unchecking the **Enable SMS Anti-Spam** box.
3. Specify whether you allow receipt of SMS message from phone numbers not included into either list by checking or unchecking the **Receive SMS from: From unknown senders'** box.
4. Specify whether you allow receipt of SMS message from phone numbers in your contact list by checking or unchecking the **Receive SMS from: From people from Contact List** box.

### 2.2.5.1. Editing the white and the black lists

The "Black" list contains phone numbers from which the receipt of SMS messages is blocked by Anti-Spam.

The "White" list contains phone numbers from which the receipt of SMS messages is allowed.

In order to edit your black or white list, open the **Anti-Spam menu** page (see Figure 13) and select the necessary list.

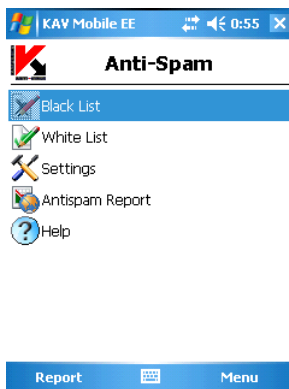


Figure 13. **Anti-Spam** menu

To edit the list use the **Menu**:

- **Insert number** – add a new record to the selected list.
- **Delete number** – delete the current record from list.
- **Edit number** - edit the current record in the list.

After you selected the **Insert number** item, specify the phone number you would like to add to the list. The number can begin with a digit or with a "+" sign and can only contain digits.

After you are done with editing the list, press **Done** to return to the **Anti-Spam menu** page.

## 2.2.5.2. Actions to be performed with messages

When you receive an SMS message from a phone number, which is not included into your black or white list, provided that you allowed receipt of messages from unknown numbers (see section 2.2.5 on page 16), Anti-Spam will display a warning on the mobile device display (see Figure 14).

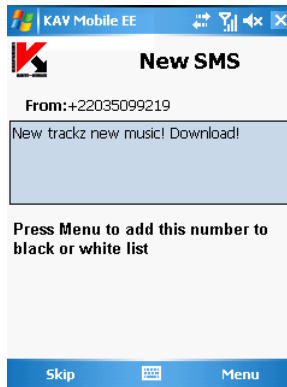


Figure 14. Anti-Spam warning

You can use **Menu** to select one of the following actions to be performed with the message:

- **Add to White List** – allow message receipt and add sender's phone number to white list.
- **Add to Black List** – block message receipt and add sender's phone number to black list.

In order to allow the receipt of the message press the **Skip** button. In this case the sender's phone number will not be added to either list.

Information about blocked messages will be added to the application log. To review the log, open the **Anti-Spam menu** tab and press the **Report** button or select the **Anti-Spam Report** item on the same tab. This report can also be accessed from the **Information** tab (see section 2.2.7 on page 20).

## 2.2.6. Updating the anti-virus bases

Kaspersky Anti-Virus detects viruses using the records from its anti-virus bases containing descriptions of all currently known malicious programs. It is extremely important to keep your smartphone safe by updating the anti-virus databases frequently.

You can update the database manually or schedule an update. In order to configure and start the update, use the **Updater menu** tab (see Figure 15). The update is performed via internet from the Kaspersky Lab's servers.

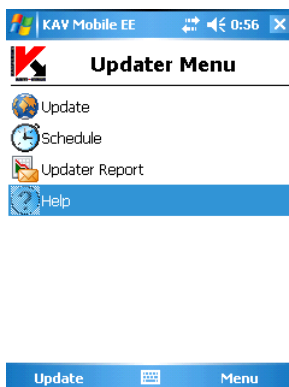


Figure 15. The **Updater menu** tab

Information about the database updates is recorded in the log. To review the log, open the **Updater menu** tab and select the **Updater Report** item. This report can also be accessed from the **Information** tab (see section 2.2.7 on page 20).

*In order to manually start updating the anti-virus bases from the Kaspersky Lab's update servers:*

1. Start Kaspersky Anti-Virus (see section 2.2.1 on page 9) and switch to the **Updater menu** tab.
2. Select **Update** in order to start the updating process.

*In order to configure a schedule for automatic updating of the anti-virus bases:*

1. Start Kaspersky Anti-Virus (see section 2.2.1 on page 9) and switch to the **Updater menu** tab.
2. Select **Schedule** in order to switch to editing the automatic update settings.
3. Specify the frequency of the updates by modifying the value of the **Update** setting:
  - **Daily** – perform the update every day. Additionally, specify the **Time** for the updates to be performed.
  - **Weekly** – perform the update every week. Additionally, specify the **Day of week** and the **Time** for the updates to be performed.
  - **Manual** - the scan will only be started manually by the user.

You can look up the **Information** tab for the release date of the anti-virus bases currently installed on the mobile device and the number of virus signatures. In order to do it select the **About AV bases** item on the tab.

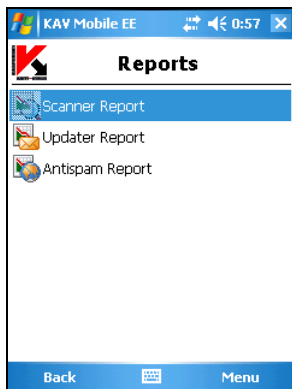
## 2.2.7. Receiving reports about the application's operation

Reports about the application's operation are collected in the **Reports** item on the **Information** tab. You can receive a report about any task performed by Kaspersky Anti-Virus:

- anti-virus scan;
- use of anti-spam;
- updating anti-virus bases.

*For example, in order to view a report about anti-virus scan, do the following:*

1. Start Kaspersky Anti-Virus (see section 2.2.1 on page 9).
2. Select the Reports item in the Information tab (see Figure 16).
3. Select a real-time protection report in the window that will open.

Figure 16. The **Reports** tab

## 2.3. Removing the program

To remove Kaspersky Anti-Virus:

1. Disable self-defense (see 2.2.3 on p. 11 for details);

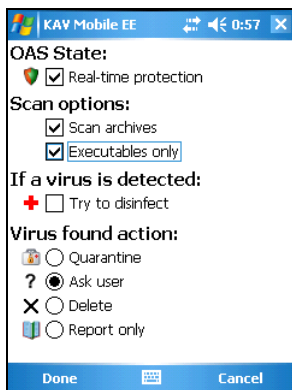


Figure 17. Disabling self-defense

2. Exit Kaspersky Anti-Virus. To do so select **Exit** in program menu (see Figure 18).

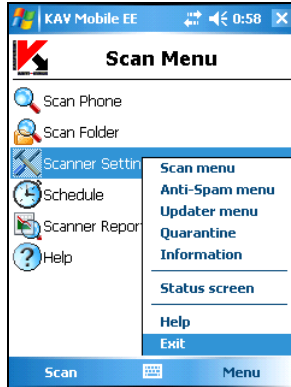


Figure 18. Exiting program

3. Remove program. To do so:

- Click the **Start** button, select **Settings** and then select **Remove programs** (see Figure 19):

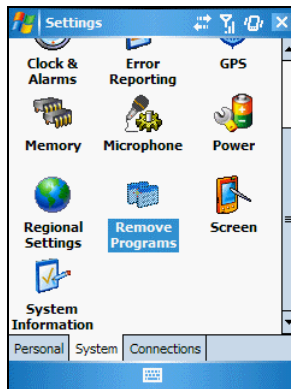


Figure 19. Remove program start

- Select **Kaspersy Anti-Virus Mobile** in the list of installed applications and then click the **Remove** button (see Figure 20).

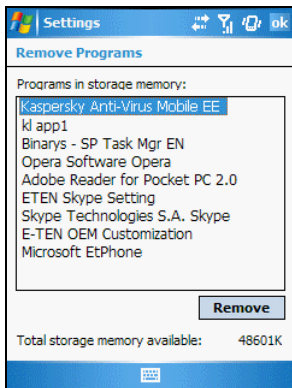


Figure 20. Program selection

- To confirm removing click **Yes** (see Figure 21).

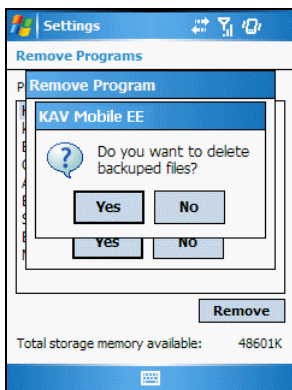


Figure 21. Removing program confirmation

---

# CHAPTER 3. MANAGING THE APPLICATION USING 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.

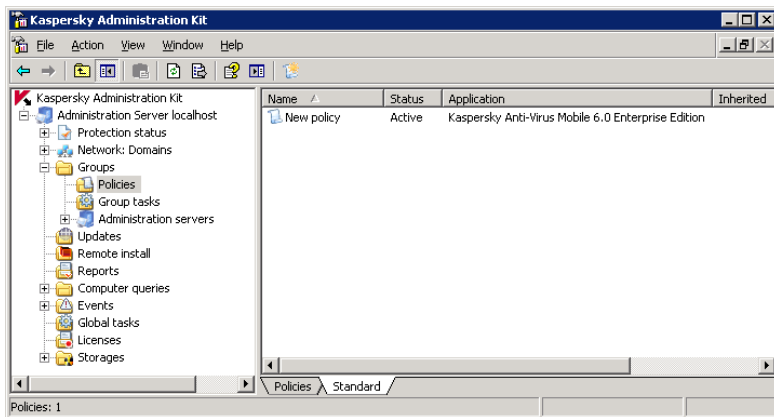


Figure 22. Kaspersky Administration Kit Administration Console

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 Anti-Virus settings in a group of the logical network. A policy allows managing the functionality of the application as it contains multiple settings of Kaspersky Anti-Virus.

A policy may also include a set of restrictions imposed on modification of the specified settings during the application configuration. These restrictions are

specified through the Kaspersky Administration Kit interface if the user has the administrator's rights.

**Note:**

In order to move the mobile device into the administration group open the **Administration Console**, switch to the **Network** container and configure it to reflect the domains. After you install the Anti-Virus all mobile devices will be placed into the **PDAGroup** group when the network is polled.

In order to make sure that Kaspersky Administration Kit detects mobile devices, check the **Open port for mobile devices** box on the **Settings** tab in the Administration Server's properties.

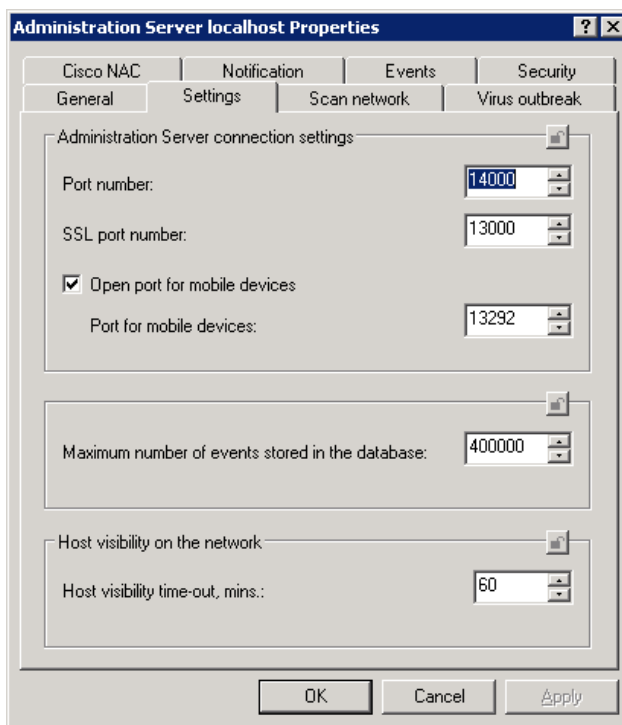


Figure 23. The **Settings** tab

## 3.1. Managing policies

This section contains information about creation and configuration of the policy settings for Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.


### 3.1.1. 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.

#### Attention!

On each step of a policy creation the settings you specified can be locked using the  button. If the lock on the button is closed, then when policy is used later on the mobile devices, 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 application **Kaspersky Anti-Virus Mobile 6.0 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 the anti-virus scan settings

During this step you will define the anti-virus scan settings to be used for scanning the mobile device: the scan scope and the schedule according to which the scan will be performed. You will also define whether the real-time protection mode will be enabled.

In order run the mobile device in the real-time protection mode check the **Enable real-time protection** box (see Figure 24). As the result, real-time protection will be enabled at the moment the device is turned on and will remain enabled until the device is turned off.

You can use the **On-demand scan** block in order to select the scan scope through selecting the file types to be scanned and to indicate whether attempts to disinfect infected objects will be made:

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

- **Scan archives** - scan files packed into archives.
- **Attempt to disinfect the infected object** – attempt to disinfect an infected object. Not all objects can be disinfectied.

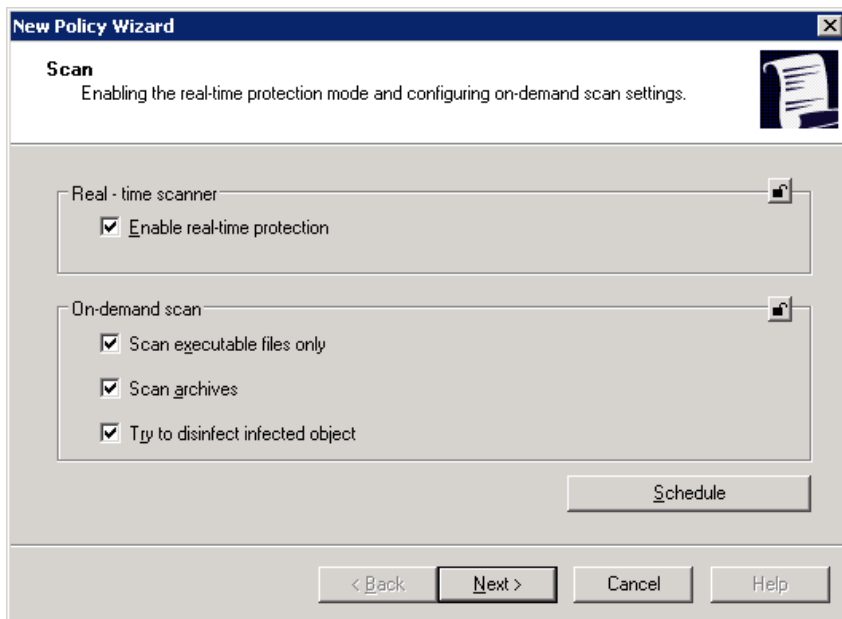


Figure 24. Configuring the anti-virus scan settings

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 **Start time** group of fields.
- **Weekly** – the action will be performed on certain weekdays. In the **Start 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. Selecting the update source

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

In the corresponding field in the **Update source** block (see Figure 24) specify the address of the update source. Only Kaspersky Lab's update servers can be used as the update source.

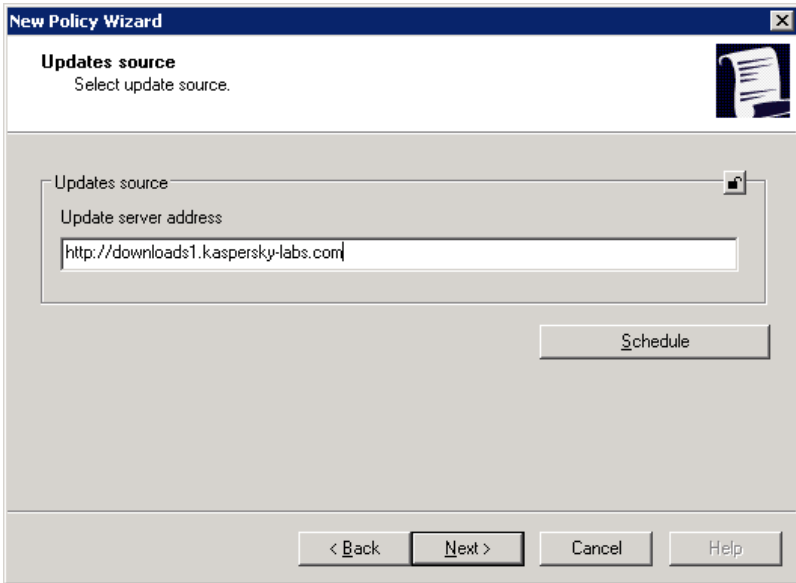


Figure 25. Selecting the update source

You can also specify a schedule for downloading updates. 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 **Start time** group of fields.
- **Weekly** – the action will be performed on certain weekdays. In the **Start 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 4. Specifying additional settings

During this step you can specify the Anti-Spam module settings and the synchronization period with the Administration Server.

Configure the Anti-Spam module settings in the **Anti-Spam** block (see Figure 26). If you check the box **Enable anti-spam protection**, Anti-Spam will analyze incoming messages for spam according to the following criteria:

- **Deliver messages from numbers in the contact list** – a criterion based on which it is determined whether numbers belong to the "white" list. Messages from the "white" list numbers are always delivered to the user.
- **Block messages from numbers not contained in the "white" list and messages with non-specified sender's number** – a criterion based on which messages will not be delivered to the user.

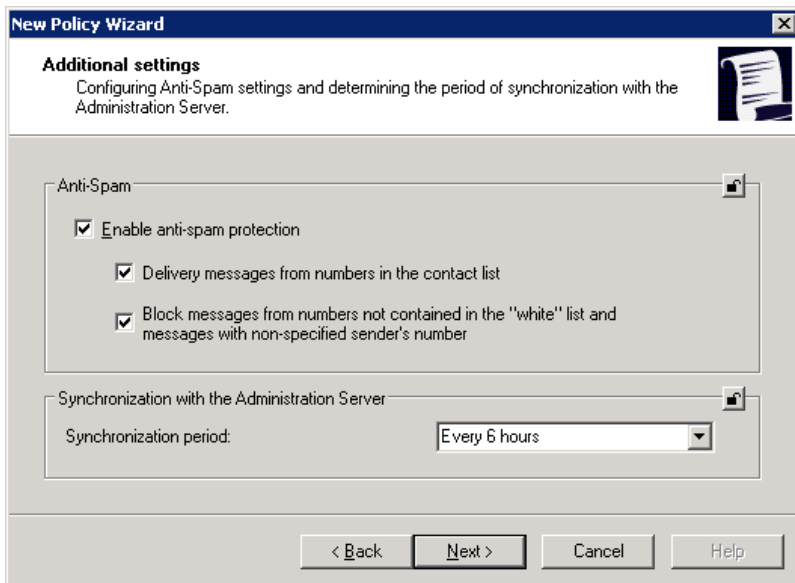



Figure 26. Additional application settings

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

## Step 5. Completing the policy creation

The last screen of the wizard informs about the successful completion of the policy creation process (see Figure 27).

Upon the completion of the wizard policies for Kaspersky Anti-Virus Mobile 6.0 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 activated on the mobile device at the time of the first synchronization of the client with the server.

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.

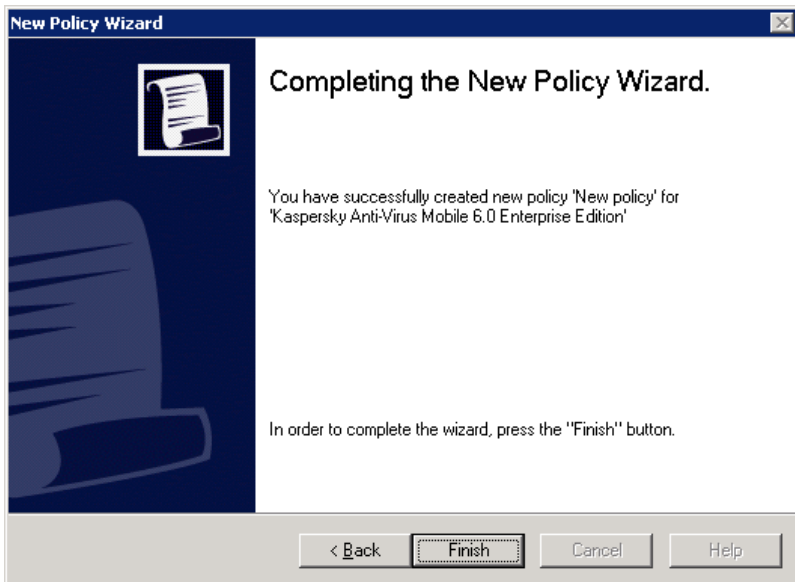


Figure 27. Completing the policy creation process

### 3.1.2. 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 of computers in 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 Anti-Virus Mobile 6.0 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 Anti-Virus Mobile 6.0 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.

### 3.1.2.1. Viewing information about the application

The following information about the policy is displayed in the **General** tab (see Figure 28): policy name, name of the application for which it is created, application version, date and time of the policy creation, date and time of its last modification.

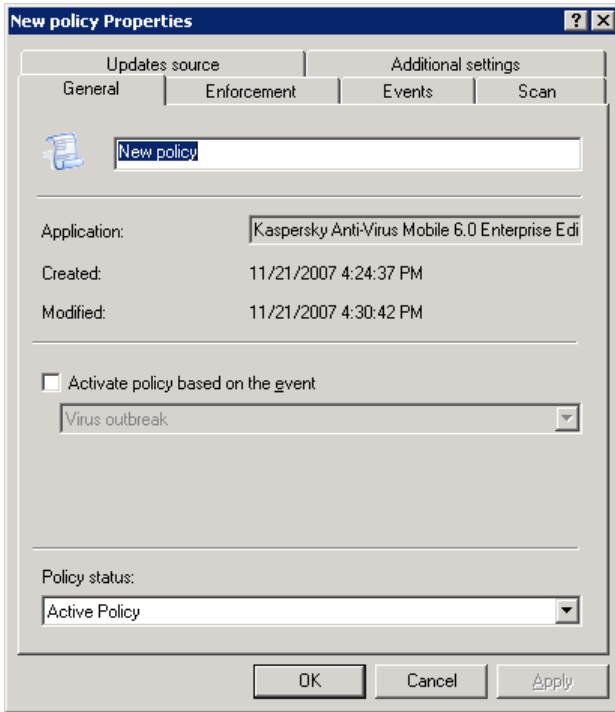


Figure 28. The **General** tab

In this dialog box you can modify the name of the policy, active or inactive it or configure activation of the policy when a certain event occurs.

### 3.1.2.2. Viewing results of the policy application

The **Enforcement** tab (see Figure 29) displays reference information about the application of the policy on the mobile devices of the group and the number of devices on which:

- the policy is not defined;
- applied;
- not applied yet;
- the policy could not be applied due to an error.

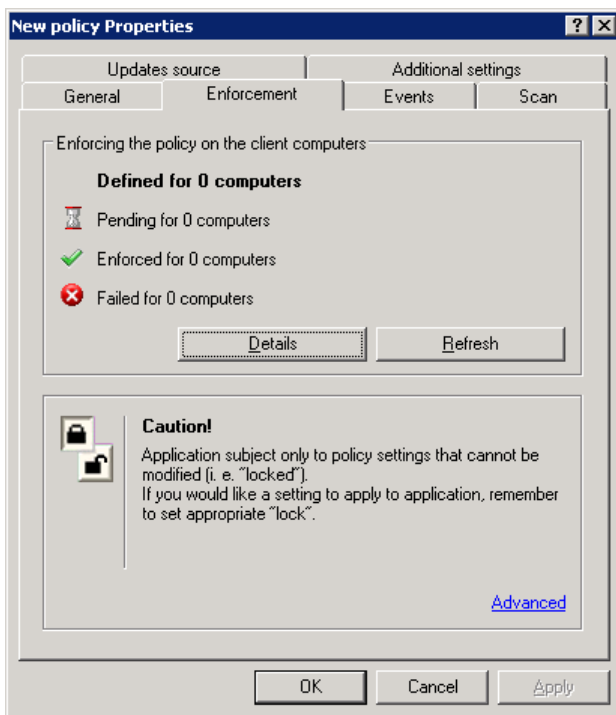


Figure 29. The **Enforcement** tab

Detailed information about results of the policy application on each client computer of the group can be viewed in the dialog box which opens using the **Details** button (for more details see Kaspersky Administration Kit 6.0 Administrator's Guide).

### 3.1.2.3. Configuring settings of registration of the application operation settings

During its operation Kaspersky Anti-Virus generates a certain set of events. Each event has a characteristic reflecting the level of its importance. There are four levels of importance: critical event, failure, warning and informational message.

Events of the same type may be of different importance level depending on the situation in which an event has occurred.

The **Events** tab (see Figure 30) displays the types of events occurring during the operation of the application and registered in the report as well as the location

where the report is saved and the administrator's and/or other user's notification mode.

In order to view the types of events select the required importance level from the **Importance level** drop-down list. Event types for the selected level will be displayed in the information field below.

For each event you can specify the possibility to be included into the report and configure administrator's notification about its occurrence.

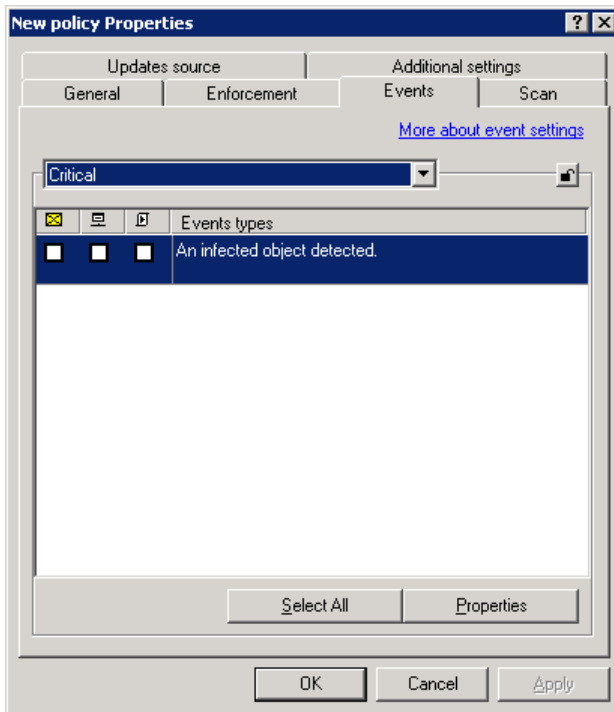


Figure 30. The **Events** tab

For detailed description of the rest of the settings available from the **Events** tab see Kaspersky Administration Kit 6.0 Administrator's Guide.

### 3.1.2.4. Defining anti-virus scan settings

The **Scan** tab (see Figure 31) is used to define the on-demand scan parameters: scan scope, actions to be performed on the infected objects, schedule according

to which the scan will be run. Also this tab will be used to determine whether the real-time protection mode will be enabled.

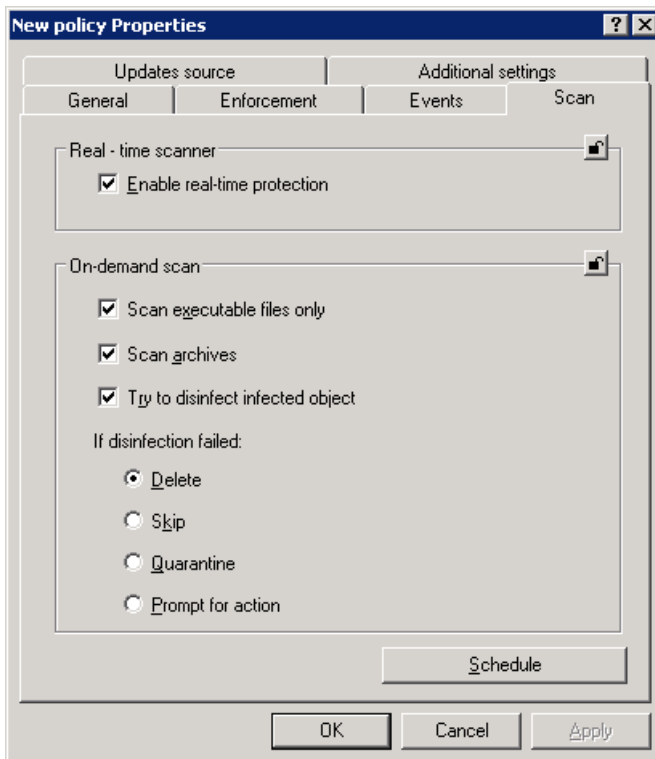


Figure 31. The **Scan** tab

In the **Action to be performed with infected object** block specify action to be performed once an infected object is detected:

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

Other parameters are similar to those described above in section 3.1.1 on page 26.

### 3.1.2.5. Selecting the Kaspersky Anti-Virus bases update source

The **Updates source** tab (see Figure 32) is used to specify the update source from which the anti-virus database updates will be downloaded. This tab is also used to configure the schedule according to which updates will be performed.

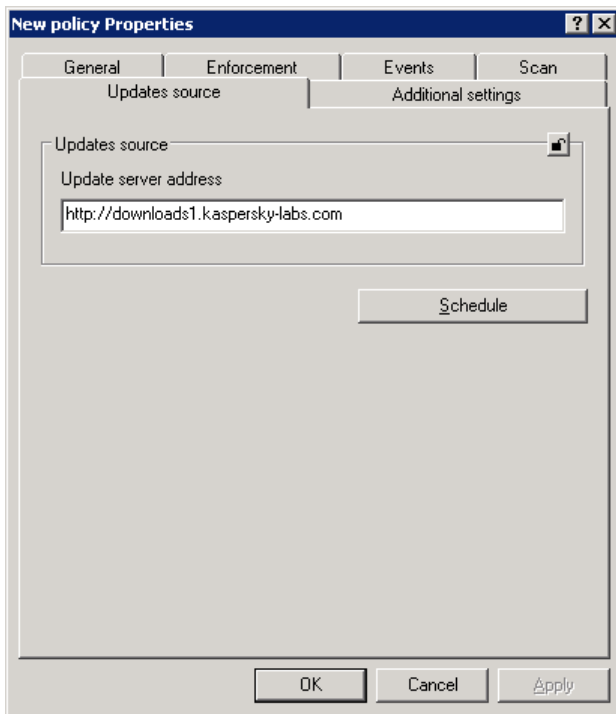


Figure 32. The **Updates source** tab

### 3.1.2.6. Specifying additional settings

The **Additional settings** tab (see Figure 33) is used to configure the Anti-Spam settings and to determine the frequency of connection with the Administration Server.

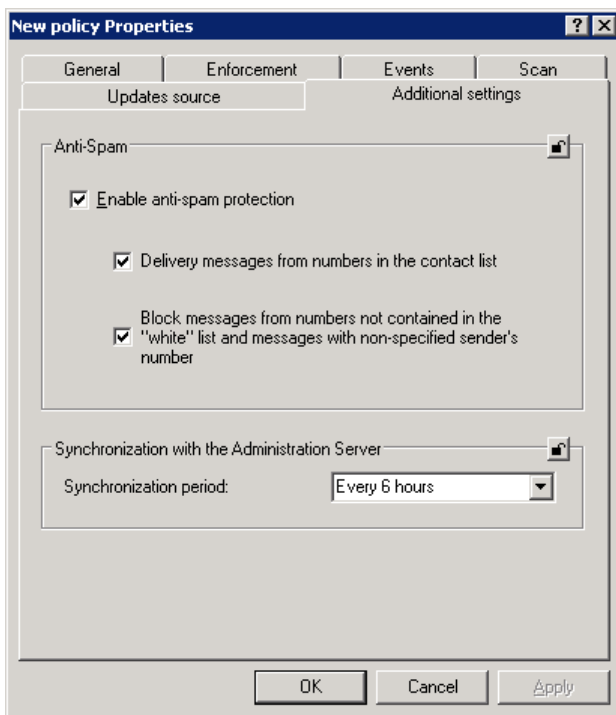


Figure 33. The **Additional settings** tab

## 3.2. Managing application settings

Using the application settings you can modify the settings of Kaspersky Anti-Virus for individual mobile devices in a group or for a local mobile device on which the application is installed. You can modify only those settings which are not locked by a policy (for details see section 0 on page 25).

*In order to edit the application settings:*

1. Select the folder with the name of the group which includes the mobile device in the **Groups** folder.
2. In the result pane select a device for which you wish to modify the application settings. Select the **Properties** command in the shortcut menu or the **Actions** menu.
3. This will open dialog box **Properties: Computer name** in the main application window. Select the **Applications** tab (see Figure 34).

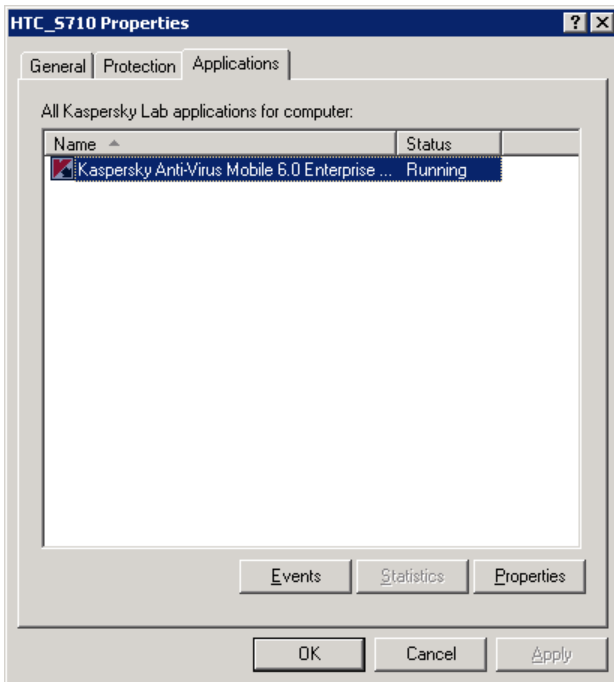


Figure 34. The mobile device properties viewing window.  
The **Applications** tab

4. Select application **Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition**. The following buttons are located in the bottom part of the window:
  - **Events** – review the list of events in the application's operation which occurred on the mobile devices and registered on the Administration Server.
  - **Statistics** – review the statistical information about the application's operation.
  - **Properties** – configure the application in window Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition application settings that will open

### 3.2.1.1. Viewing application information

The **General** tab (see Figure 35) is used to view information about Kaspersky Anti-Virus Mobile 6.0 Enterprise Edition.

The top part of the window contains the name of the installed application, information about the version, installation date, its status (running or stopped on the mobile device) and information about the status of Kaspersky Anti-Virus bases.

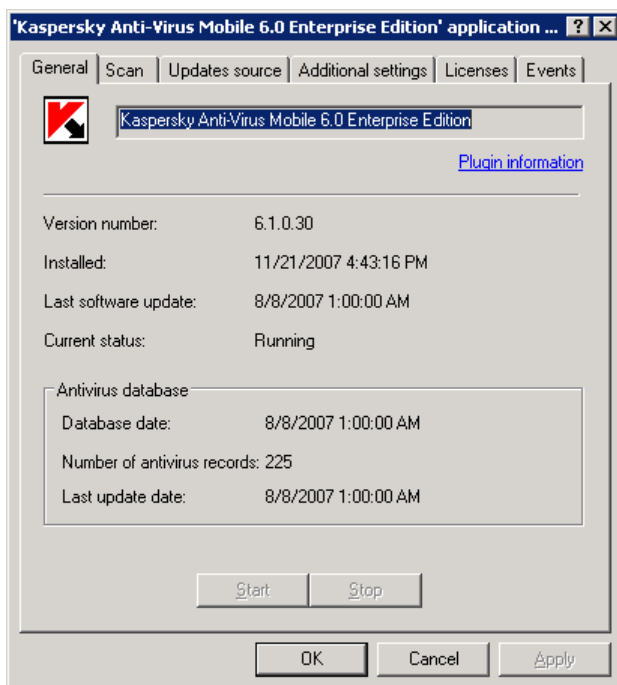
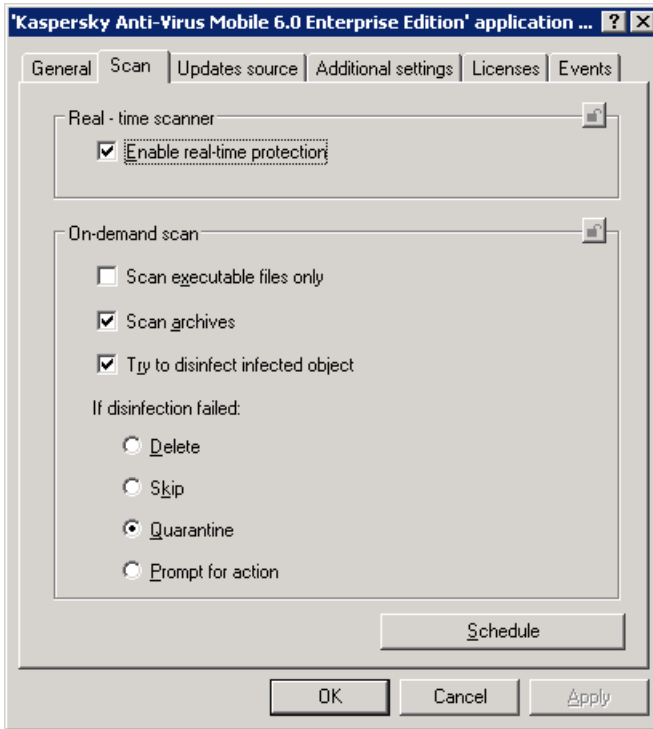


Figure 35. The application properties configuration dialog box. The **General** tab.

### 3.2.1.2. Viewing information about the anti-virus application settings

The **Scan** tab (see Figure 36) can be used to view information about the on-demand scan task: scan scope, action to be performed on the objects and about the schedule according to which the scan will be run. This tab also contains information whether the real-time protection is enabled on the mobile device.

Figure 36. The **Scan** tab

### 3.2.1.3. Viewing information about the update source

The **Updates source** tab (see Figure 37) can be used to obtain information about the server from which according to the settings updates for the particular mobile device will be downloaded and according to which schedule updates will be performed on the selected mobile device.

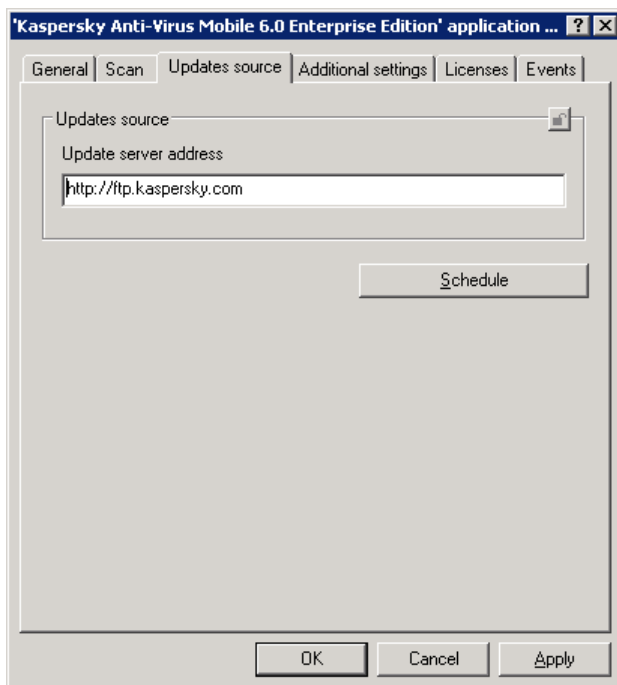


Figure 37. The Updates source tab

### 3.2.1.4. Viewing information about additional settings

The **Additional settings** tab (see Figure 38) can be used to obtain information about the Anti-Spam settings and about the frequency of communication with the Administration Server.

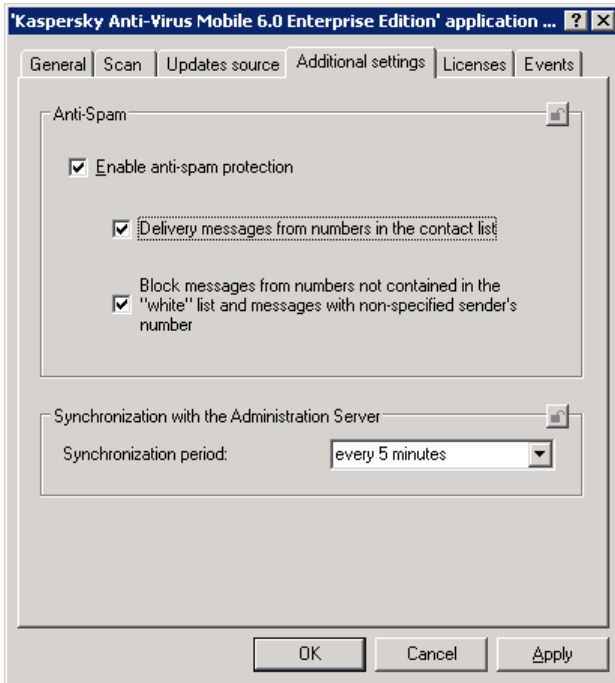
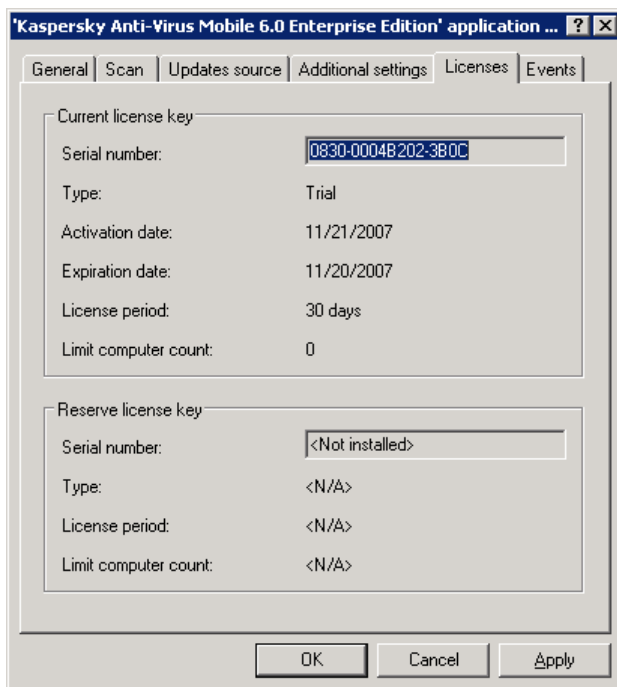


Figure 38. The **Additional settings** tab

### 3.2.1.5. Viewing information about the keys

The **License** tab (see Figure 38) contains information about the current or the backup key installed on the particular mobile device. It also contains information about the current key, its license period and the license restriction. For the current key it also contains information about the activation date and the expiration date.

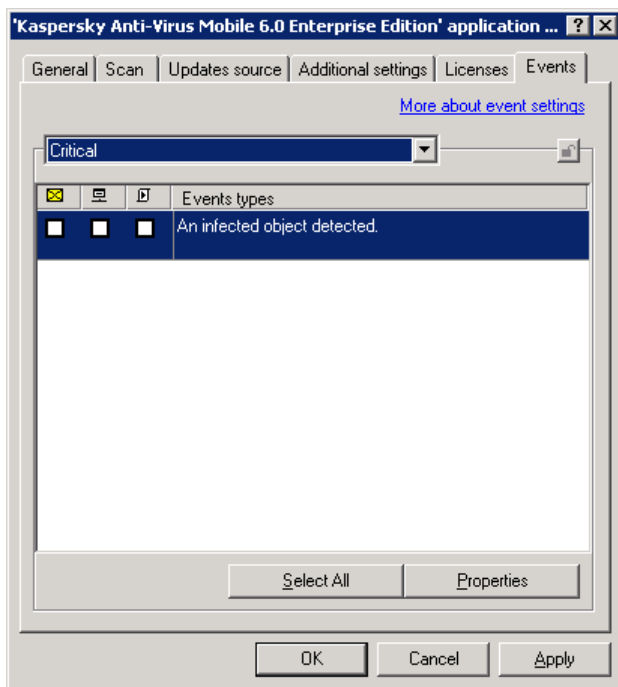
Figure 39. The **Licenses** tab

### 3.2.1.6. Viewing information about events

During its operation Kaspersky Anti-Virus generates a certain set of events. Each event has a characteristic reflecting the level of its importance. There are four levels of importance: critical event, failure, warning and informational message.

Events of the same type may be of different importance level depending on the situation in which an event has occurred.

The **Events** tab (see Figure 40) displays the types of events occurring during the operation of the application and registered in the report as well as the location where the report is saved and the administrator's and/or other user's notification mode.

Figure 40. 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 Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, email systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

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

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

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

### Kaspersky® OnLine Scanner

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

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

### Kaspersky® OnLine Scanner Pro

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

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

## Kaspersky Anti-Virus® 7.0

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

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

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

Proactive protection offers the following features:

- **Controls modifications within the file system.** The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitors processes in random-access memory.** Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.
- **Monitors changes in OS registry** due to internal system registry control.
- **Hidden Processes Monitor** helps protect from malicious code concealed in the operating system using rootkit technologies.
- **Heuristic Analyzer.** When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.
- **Performs system restore** after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

## Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 is an integrated solution for protection of personal computers against the major information- threats (viruses, hackers,

spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection:** anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.
- **Proactive protection:** the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

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

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

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

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

- Recognition of spam sent in image files

### **Kaspersky Anti-Virus for File Servers**

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

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

Features and functionality:

- *Protects server file systems in real time: All server files are scanned when opened or saved on the server*
- *Prevents virus outbreaks;*
- *On-demand scans of the entire file system or individual files and folders;*
- *Use of optimization technologies when scanning objects in the server file system;*
- *System rollback after virus attacks;*
- *Scalability of the software package within the scope of system resources available;*
- *Monitoring of the system load balance;*
- *Creating a list of trusted processes whose activity on the server is not subject to control by the software package;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Saving backup copies of infected and deleted objects in case you need to restore them;*
- *Quarantining suspicious objects;*
- *Send notifications on events in program operation to the system administrator;*
- *Log detailed reports;*
- *Automatically update program databases.*

## Kaspersky Open Space Security

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

The suite includes four programs:

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

Specifics on each program are given below.

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

Features and functionality:

- *Comprehensive protection from viruses, spyware, hacker attacks, and spam;*
- *Proactive Defense from new malicious programs whose signatures are not yet added to the database;*
- *Personal Firewall with intrusion detection system and network attack warnings;*
- *Rollback for malicious system modifications;*
- *Protection from phishing attacks and junk mail;*
- *Dynamic resource redistribution during complete system scans;*
- *Remote administration of the software package, including centralized installation, configuration, and administration;*
- *Support for Cisco<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> Active Management, Intel<sup>®</sup> vPro<sup>™</sup>)*;
- *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 <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a> Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">www.kaspersky.com/helpdesk.html</a>
General information	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> Email: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>

---

# 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 ANTI-VIRUS 6.0 MOBILE 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’S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD’S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

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

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

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

1. *License Grant.* Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby

grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes.

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

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

1.1.2 The Software protects computer against viruses 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 computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

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

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

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

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

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

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

## 2. Support.

1. Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of purchasing on:
  - (a) payment of its then current support charge, and;
  - (b) Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.
  - (c) Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders assistance in Software activation and registration of the End User only.
2. By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on [www.kaspersky.com/privacy](http://www.kaspersky.com/privacy), and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.
3. 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.
4. "Support Services" means:
  - Hourly updates of the anti-virus database;
  - Updates of network attacks database;
  - Updates of anti-spam database;
  - I. Free software updates, including version upgrades;
  - II. Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
  - III. Virus detection and disinfection updates in 24-hours period.
5. Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the

official Kaspersky Lab website ([www.kaspersky.com](http://www.kaspersky.com)) installed on your computer.

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

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

5. *Limited Warranty.*

- (i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.
- (ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.
- (iii) Kaspersky Lab does not warrant that this Software identifies all known viruses and spam letters, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) Kaspersky Lab does not warrant that this Software provides protection after expiring date (see section.2 (i))
- (v) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.
- (vi) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b)

use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

- (vii) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

#### 6. *Limitation of Liability.*

- (i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.
- (ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):
- (a) Loss of revenue;
  - (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
  - (c) Loss of the use of money;
  - (d) Loss of anticipated savings;
  - (e) Loss of business;
  - (f) Loss of opportunity;
  - (g) Loss of goodwill;
  - (h) Loss of reputation;
  - (i) Loss of, damage to or corruption of data, or:
  - (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

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

---

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

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