

KASPERSKY LAB

Kaspersky Mobile Security 7.0

USER'S GUIDE

KASPERSKY MOBILE SECURITY 7.0

User's Guide

© Kaspersky Lab
Tel., Fax: +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
<http://www.kaspersky.com>

Revision Date: December, 2007

Table of Content

CHAPTER 1. KASPERSKY MOBILE SECURITY 7.0.....	5
1.1. Hardware and software requirements	6
1.2. Distribution kit	6
CHAPTER 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS.....	7
2.1. Installing Kaspersky Mobile Security	7
2.2. Using the application	8
2.2.1. Activating the application	8
2.2.2. Starting the application	9
2.2.3. Graphical user interface	10
2.2.4. General settings.....	11
2.2.5. Anti-virus scan and protection	12
2.2.6. Using Quarantine.....	17
2.2.7. Using the Anti-Spam and the Anti-Theft modules	19
2.2.8. Updating the application bases	26
2.2.9. Using the Firewall module	29
2.2.10. Viewing report about the application operation	30
2.3. Removing the application.....	31
CHAPTER 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE	33
3.1. Installing Kaspersky Mobile Security	33
3.2. Getting started	34
3.2.1. Activating the application	34
3.2.2. Starting the application	35
3.2.3. Graphical user interface	37
3.3. Anti-virus scan and protection.....	38
3.3.1. Real-time protection and on-demand scan	38
3.3.2. Scheduled scan	42
3.4. Using Quarantine.....	43
3.5. Using the Anti-Spam and the Anti-Theft modules.....	44
3.5.1. Anti-Spam module.....	44

3.5.2. Editing “black” and “white” lists.....	45
3.5.3. Actions to be performed with messages.....	46
3.5.4. The Anti-Theft module.....	47
3.6. Updating the application bases.....	50
3.7. Firewall.....	52
3.8. Viewing reports about the application operation.....	53
3.9. Removing the application.....	54
APPENDIX A. KASPERSKY LAB.....	58
A.1. Other Kaspersky Lab Products.....	59
A.2. Contact Us.....	69
APPENDIX B. LICENSE AGREEMENT.....	70

CHAPTER 1. KASPERSKY MOBILE SECURITY 7.0

Kaspersky Mobile Security 7.0 is designed to ensure protection of smart-phones and communicators running Symbian OS and Microsoft Windows Mobile against malware programs, unsolicited e-mail messages and performs the following functions:

- **real-time protection** of the file system of the device - interception and scan of:
 - all incoming objects transmitted using wireless connections (IR port, Bluetooth), EMS and MMS messages, during synchronization with the personal computer and downloading files using a browser;
 - files opened on the mobile device;
 - programs installed from the device's interface.
- **scanning of the file system's objects** on the mobile device or on the connected expansion cards by user's demand or according to the schedule;
- **reliable isolation of infected objects** in the quarantine storage;
- **updating of Kaspersky Mobile Security bases** used to scan for malware programs and delete dangerous objects.
- **blocking unwanted SMS and MMS messages.**
- **blocking access to or erasing user's data** in case of unauthorized actions with the device, as, for instance, theft.
- **protection of the mobile device at the network level.**

The user can use the capabilities providing flexible control of the Kaspersky Mobile Security settings, viewing the current anti-virus protection status and the event log in which the application's actions are recorded.

The application includes a menu system and supports an easy-to-use user's interface.

Note

In case a detection of a malware program, Kaspersky Mobile Security can disinfect the infected object detected (if disinfection is possible), delete it or place it into the quarantine. In this case no copies of the object being deleted will be saved.

1.1. Hardware and software requirements

Kaspersky Mobile Security is designed for installation on smartphones and communicators running one of the following operating systems:

- Symbian OS 9.1, 9.2 Series 60 UI.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

The program runs only on smartphones and communicators that support receipt and sending of SMS messages.

1.2. Distribution kit

You can purchase Kaspersky Mobile Security via internet (the application distribution kit and documentation in the electronic form). Kaspersky Mobile Security can be also purchased in mobile communication offices. For more details contact you mobile communication operator.

CHAPTER 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS

This chapter contains description of the operation of Kaspersky Mobile Security 7.0 for smartphones running Symbian version 9.1, 9.2 Series 60 UI operating system.

2.1. Installing Kaspersky Mobile Security

In order to install Kaspersky Mobile Security, perform the following steps:

1. Copy the application distribution package to your smartphone.
2. Run installation (open the cab archive with the distribution package on your smartphone).
3. To confirm the installation, select **Yes** (see Figure 1).



Figure 1. Prompt to confirm the installation

4. If the language versions of Kaspersky Mobile Security operating system do not match, a corresponding message will then be displayed on the screen. In order to proceed with the installation in Russian, press **OK**.

5. Read the text of the license agreement. If you agree to all terms of the agreement, press **OK**. To cancel the installation, press **Cancel** (see Figure 2).



Figure 2. License Agreement

Warning!

This software is not intended to be backed up/restored.

2.2. Using the application

This section contains information about configuration of the settings of the anti-virus scan and real-time protection, SMS and MMS messages filtering, smartphone anti-virus scan, the application update smartphone protection at the network level, etc.

2.2.1. Activating the application

When you run the application for the first time, the Kaspersky Mobile Security activation window (see Figure 3) will be displayed on the smartphone screen.



Figure 3. The Application activation window

Activation is necessary as without it all Kaspersky Mobile Security functions will not be available. You can receive the activation code at Kaspersky Lab's website.

Warning!

For the activation of Kaspersky Mobile Security 7.0 you must have GPRS or WLAN connection on your smartphone.

The activation code consists of Latin alphabet characters and digits (the code is case-insensitive). Enter the code into the four fields.

After you have entered the activation code, select **Start Activation** in the **Options** menu. The application will send an http query to Kaspersky Lab's activation server and will then download and install the key.

If the activation code you entered appears invalid for any reason, a corresponding message will be displayed on your smartphone's screen.

2.2.2. Starting the application

In order to start Kaspersky Mobile Security, perform the following actions:

1. Open the phone's main menu.
2. Select **KMS 7.0** and start the application using the **Open** item from the **Options** menu.

Note

When you start the application for the first time, you will be offered to enable the automatic startup function (see section 2.2.4 on page 11). If you agree, press **OK**.

After the smartphone is on a window with main Kaspersky Mobile Security components (see Figure 4) will be displayed on the smartphone's screen.

- **Real-Time Protection** - using the real-time protection mode (see section 2.2.5 on page 12);
- **Last Full Scan** – date of the last anti-virus smartphone scan.
- **Database date** – release date of the anti-virus database used by the application.
- **Anti-Spam Config.** – Anti-Spam operation mode (see section 2.2.7 on page 19).
- **Firewall level** – smartphone protection level (see section 2.2.9 on page 29).



Figure 4. The Application component status window

In order to switch to the application interface, press **OK**.

2.2.3. Graphical user interface

The graphical user interface (GUI) contains six tabs:

- Using the **Scanner** tab you can perform an anti-virus scan of the smartphone, edit the anti-virus scan and real-time protection mode and configure the auto scan schedule.
- Using the **Quarantine** tab you can manage the quarantine – a special-purpose storage for infected and suspicious objects.
- Using the **Updater** tab you can update the anti-virus database, edit the updating settings and configure the updating schedule.

- Using the **Firewall** tab you can monitor the network activities and protect smartphone at the network level.
- Using the **Miscellaneous** tab you can configure filtering of incoming SMS and MMS messages (Anti-Spam module) and block the smartphone or erase information in case the smartphone was stolen or lost (Anti-Theft module).
- Using the **Information** tab you can view application component's operation logs, general information about the application and the anti-virus bases used and edit general settings used for application's operation.

To navigate from one tab to another, use the joystick of the smartphone or select the **Open Page** item in the **Options** menu (see Figure 5).



Figure 5. The **Options** menu

In order to return to the application components status window, select the **Current Status** item in the **Options** menu.

2.2.4. General settings

Using settings in the **Information** tab in the **Settings** item (see Figure 6) you can configure the following application's functions:

- **Automatic Launch** – automatic startup mode. With the automatic startup mode active, the main application's functions will be started when the smartphone is turned on. Once you disable the automatic startup option the main functions will be stopped. If you wish your phone to be always protected with the main functions, select **Yes**.
- **Show Status Screen** determines whether the current status will be displayed at the application startup.

- **Log Size** determines the maximum log size. Once the limit has been reached, old messages of the log will be deleted to the maximum value specified in the setting.
- **Screen Backlighting** determines whether the screen will be lit during the anti-virus scan. By default the backlight option is disabled.
- **Play Sound** determines the use of the sound notification in case of certain events (detection of an infected objects, message about an application status, etc.) Select **Yes** if you wish to use the sound notification.
- **Vibration** determines whether the smartphone will vibrate when an infected object is detected. By default vibration is enabled.



Figure 6. The **Settings** menu

In order to edit the values of the settings, use the smartphone's joystick or select the **Change** item in the **Options** menu.

2.2.5. Anti-virus scan and protection

Using the **Scanner** tab you can perform anti-virus scan of the entire file system and the memory of the smartphone or of an individual folder or file. You can also modify the settings of the anti-virus scan and of the real-time anti-virus protection, view the report about the scan results and configure the automatic scan start schedule.

2.2.5.1. Real-time protection and on-demand scan

Real-time protection is the mode of operation in which the resident part of Kaspersky Mobile Security is constantly loaded in the smartphone's RAM and monitors all data including the incoming data received by the smartphone.

Real-time protection is started since the moment the smartphone is turned on and works until it is turned off (if the use of this mode was not disabled by the settings).

Kaspersky Mobile Security also allows to perform a full scan of the smartphone's file system including the analysis of objects located on the connected memory expansion cards.

Information about the results of the real-time protection and of the on-demand scan will be recorded in the report. In order to view the report, select the **Log** item in the **Scanner** tab.

In order to start the real-time protection use mode, perform the following:

1. Select the **Settings** item in the **Scanner** tab.
2. Enable / disable the mode of using the real-time protection by setting the **Real-Time Protection** setting certain value to a corresponding value.

In order to change the on-demand scan settings, perform the following:

1. Select the **Settings** item in the **Scanner** tab.
2. Define the scan area in the **Scan Mask** block by selecting the file types to be scanned:
 - **All files** – scan all files.
 - **Executable files** – scan only executable program files (for example *.exe, *.sis, *.mdl, *.app).
3. Determine the action to be performed when an infected object has been detected (the **Virus Found Action** setting).

If you wish a prompt for action to be displayed on the smartphone screen when an infected object is displayed, select the **Ask User** value.

For automatic deletion without a notification of the user, select the **Auto Delete** value.

If you wish the detected objects to be automatically moved to the quarantine, select **Quarantine**. Quarantining the infected objects is the default action.

4. Enable / disable the scan of the smartphone's ROM memory (the **ROM scan** setting).

In some situations the ROM memory may become vulnerable for malware programs. In order to allow the scan of the ROM memory by Kaspersky Mobile Security, select the **Yes** value.

5. Enable / disable unpacking of SIS and ZIP archives (the **Unpack archives** setting).

If you wish Kaspersky Mobile Security to unpack SIS and ZIP archives during the scan, select **Yes**. If archives do not need to be unpacked during the scan, disable this function by selecting **No**.

6. Enable / disable new card scan mode (the **Scan New Card** setting).

If you want Kaspersky Mobile Security to scan a new card in the background mode, select **Auto Scan**. In order to disable the automatic scan of flash cards, select **Disable**. If you wish Kaspersky Mobile Security to display a prompt for the scan of a new card each time such card is installed, select **Ask User**.

7. Enable / disable the display of the protection icon (the **Protection icon** setting).

Select the **Always** value in the corresponding item of the menu if you wish the application icon to be always displayed on the smartphone's screen when the real-time protection is enabled. If you wish the icon to be displayed only in the smartphone's menu, select **Only in Menu**. If you do not wish this icon to be displayed, select **Off**.

Note

In order to edit the values of the settings, use the smartphone's joystick or select the **Change** item in the **Options** menu.

By default the application uses the settings recommended by Kaspersky Lab's specialists. If you wish to return to the recommended settings while you are using the application, open the **Scan** tab and select the **Restore** item from the **Options** menu.

In order to create a scan schedule, perform the following actions:

1. Start Kaspersky Mobile Security (see section 2.2.2 on page 9).
2. Using the **Scanner** tab (see Figure 7) select the **Scan All** item if you wish to scan the entire file system of the smartphone or **Scan folder** if you wish to scan an individual folder.

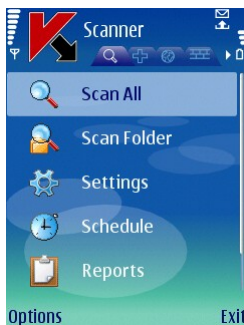


Figure 7. The **Scanner** tab

If you selected the **Scan Folder** item, you will be transferred to the window displaying the smartphone's file system. In order to navigate through the file system use the joystick buttons of your smartphone. In order to scan a folder, move the cursor to the folder you wish to scan and select the **Scan** item from the **Options** menu.

After the scan is started, the scan process window will open in which the current status of the task will be displayed: the number of scanned objects, the path to the object being scanned at the time and the percentage indicator of the progress (see Figure 8).

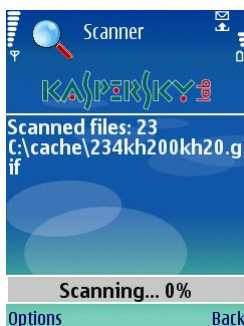


Figure 8. The **Scan progress** window

If an infected object is detected, you will be offered to either delete an infected file (**Delete** action), quarantine it (**Quarantine** action) or leave it intact (**Skip** action).

Warning!

A prompt for the action to be performed with the object will only be displayed if the **Action** setting of the scan is assigned value **Ask User** (for more details see section 2.2.5.1 on page 13).



Figure 9. Notification about the virus detection

Once the scan is complete the general statistics about detected and deleted malware objects will be displayed.

If you wish the screen backlight to be constantly on during the scan, switch to the **Information** tab, open the **Settings** menu and select the **On** value for the **Screen Backlighting** setting. By default, if no smartphone keys are pressed, the backlight will turn off automatically to save the battery life.

2.2.5.2. Scheduled scan

Kaspersky Mobile Security allows the user to create the schedule for the automatic smartphone scan. The scan is performed in the background mode. When detecting an infected object an action specified in the scan settings will be performed with such object (see section 2.2.5.1 on page 13).

By default scheduled scan is disabled.

In order to configure scheduled scan:

in the **Scanner** tab select the **Schedule** item and configure the **Auto Scan** settings (see Figure 10):

- **Daily** - the scan to be performed every day. Specify the **Scan Time** in the entry field.
- **Weekly** - the scan will be performed once a week. Specify the **Auto Scan Day** and **Auto Scan Time**.

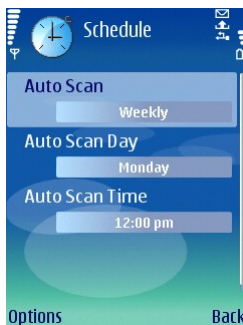


Figure 10. The **Schedule** menu

2.2.6. Using Quarantine

Infected objects placed into the quarantine do not impose any threat for the smartphone and can be deleted or restored later.

Detected infected objects can be quarantined by the application automatically or after your confirmation.

In order to configure automatic quarantining of infected objects by the application, switch to the **Scanner** tab, select the **Settings** item and select **Quarantine** as the value for the **Virus Found Action** setting.

If you selected **Ask User** as the action to be performed, then, when an infected object is detected, Kaspersky Mobile Security will offer that you either delete this object or quarantine it.

Access to the main quarantine functions is provided from the **Quarantine** tab (see Figure 11).



Figure 11. The **Quarantine** menu

In order to view the list of all objects in the quarantine, select **Quarantine** (see Figure 12).

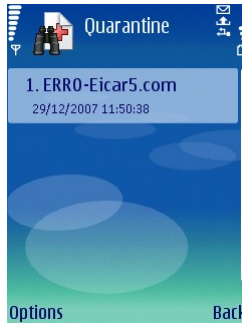


Figure 12. Infected quarantined objects

The **Options** menu accessible from the quarantine view window allows the user:

- To view detailed information about each object in the quarantine (**View Details**).
- Delete the selected object (**Remove File**).
- Clear the quarantine by deleting all quarantined objects (**Remove All**).
- Restore the current object from the Quarantine to its original folder (**Restore File**).
- View Quarantine Help (**Help**).

In order to configure the quarantine settings use the **Settings** menu in the **Quarantine** tab (see Figure 13).



Figure 13. Quarantine settings

The **Quarantine Size** setting determines the maximum number of infected objects which can be stored in the quarantined. The possible values are **20**, **50** or **100** files.

The **Store Limit** setting determines the period of time during which the infected objects can be stored in the quarantine. After this period elapses, the infected objects will be automatically deleted.

Note

In order to restore the quarantine settings recommended by Kaspersky Lab's specialists select **Restore** from the **Options** menu.

2.2.7. Using the Anti-Spam and the Anti-Theft modules

The Anti-Spam module is designed to ensure protection of your smartphone against unsolicited SMS and MMS messages.

Filtering is based on the use of "black" and "white" lists. Incoming messages received from phone numbers that had been added to the "black" list are blocked by Anti-Spam. Messages received from numbers that had been added to the "white" list, are not blocked.

The Anti-Theft is designed to ensure blocking the smartphone and erasing information stored in its memory in case it is lost or stolen.

2.2.7.1. Anti-Spam work modes

In order to configure the Anti-Spam work mode, switch to the **Miscellaneous** tab and select **Anti-Spam**, then select the **Settings** item. Select one of the following modes using the **Anti-Spam** setting:

- **Enable.** 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 generate a warning to the user and will offer to block or allow receipt of the message and to include this phone number into the "white" or "black" list.
- **B/W Lists Only.** In this mode Anti-Spam will filter incoming messages only based on the data contained in the "white" and "black" lists. Receipt of messages from numbers not included into either list will be allowed without user's confirmation.

- **Disable.** In this mode Anti-Spam is disabled. No filtering of incoming messages is provided.

2.2.7.2. Editing “black” and “white” lists

"Black" and "White" lists contain records with phone numbers, SMS and/or MMS from which will be block or passed by Anti-Spam. Information about blocked or deleted messages will be entered in the **Log** section.

Note

Messages not included into either list will not be blocked!

In order to edit the "black" or the "white" list, switch to the **Anti-Spam** tab (see Figure 14) and select the corresponding list.

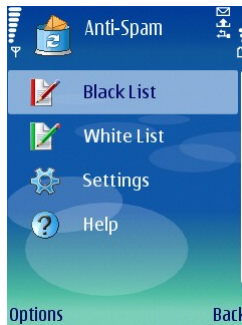


Figure 14. The **Anti-Spam** menu

To edit the list use the **Options** menu:

- **Add Record** – add a new record to the list.
- **Edit Record** – edit the current record.
- **Remove Record** – delete record from the list.
- **Remove All** – clear the list by deleting all records.
- **Help** – view Help on managing the list.

When you select the **Add record** or the **Edit record** item, you will be offered to specify the following record's parameters:

- **Message type:** Specify which types of incoming messages will be blocked (for the "black" list) or allowed (for the "white" list). Allowable values: **SMS only**, **MMS only** and **All messages**.

- **Phone number.** Specify the phone number for which receipt of messages will be blocked or allowed. When specifying a number, you can use masks "?" and "*".
- In the **Text** field specify the text detection of which by the application in the received message will cause the application to perform the following actions:
 - the message in which such text specified for the "white" list is found will be allowed to pass;
 - the message in which such text specified for the "black" list is found will be blocked;

Message analysis will be performed in the following order:

- check if the number is included into the "black" list;
- check if the number is included into the "white" list;
- check if the message text is included into the "black" list;
- check if the message text is included into the "white" list;

If the message meets any of these conditions, further analysis will not be performed and the message will be either allowed to pass or it will be blocked depending on whether it is included into the "black" or the "white" list.

After you have specified these settings, press the **Back** button on order to save the record and switch to the list view window (see Figure 15).



Figure 15. The "black" list

2.2.7.3. Anti-Spam settings

To configure the Anti-Spam settings, switch to the **Anti-Spam** tab and select the **Settings** item (see Figure 16).



Figure 16. Anti-Spam settings

The following Anti-Spam settings are accessible in the **Settings** menu:

- **Allow Contacts List.** If the setting is assigned value **Yes**, Anti-Spam will not block receipt of messages from phone numbers contained in your phone book. If this option is disabled (**No** value), Anti-Spam will perform filtering depending on whether the phone number is included in to the "white" or "black" list.
- **Add outgoing.** If the setting is assigned value **Yes**, all phone numbers to which you send SMS or MMS messages will be automatically added to the "white" list. To disable this option, select **No**.
- **Block non-numeric.** If this setting is assigned value **No**, Anti-Spam will not block all incoming messages from non-numeric numbers. To enable this option, select **Yes**.
- **Distinguish types:** If this setting is assigned value **No**, then for new records created by Anti-Spam in the "white" or in the "black" list, value **All messages** will be used to determine the message type (for more details about settings of records included into the lists see 2.2.7.2 on page 20), otherwise records will be created for certain types of messages (SMS or MMS).

Note

This setting affect only records created by Anti-Spam in one of the following situations:

- adding outgoing numbers to the "white" list (setting **Add outgoing** is enabled);
- adding new phone numbers from which messages are received to one of the lists (see section 2.2.7.4 on page 23).

In order to edit the values of the settings, use the smartphone's joystick or select the **Change** item in the **Options** menu.

2.2.7.4. Actions to be performed with messages

When you receive an SMS or an MMS message from a phone number not found in either the "black" or the "white" list, such message will be intercepted by Anti-Spam and a warning will be displayed on the screen of the smartphone (see Figure 17).

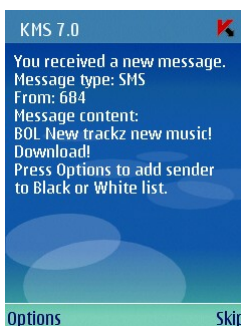


Figure 17. Anti-Spam warning

Using the **Options** menu you can select one of the following actions to be performed with the message:

- **Add to "white" list** – allow receipt of messages and add the sender's phone number to the "white" list.
- **Add to "black" list** – block messages and add the sender's phone number to the "black" list.
- **Skip** – allow the receipt of the message. In this case the sender's phone number will not be added to either of the lists.

If the **Distinguish types** setting is set to **No** in the Anti-Spam settings, then when you select the **Add to "white" list** or the **Add to "black" list** actions a record will be created in the corresponding list for all types of messages (**Message type - All messages**), otherwise the type will be determined by the type of the message received (for more details about settings of records in the lists see section 2.2.7.2 on page 20).

Information about blocked messages will be entered into the application log. In order to view the report, select the Log item in the Miscellaneous tab.

2.2.7.5. The Anti-Theft module

This module is designed to ensure protection of data stored on the mobile device against unauthorized access to it in case the device was lost or stolen.

When you access the module settings for the first time you will have to set up a password. Using this password you can obtain access to the module's settings in order to modify them. The password is required in order to prevent unauthorized access to the settings and to enable the user to block and erase information saved on the smartphone in case it is stolen or lost.

SMS-Block – allows blocking the device at the user's discretion. You can unblock the device only after you enter a password used to access the Anti-Theft module. This setting is enabled after the user of the stolen smartphone sends to this smartphone SMS: "*block:code*". In order to use this function, select **On**.

SMS-Clean allows erasing user's personal information (contact, incoming messages, personal files). This feature is triggered after the user of the stolen device sends to this device SMS: "*clean:code*". In order to use **SMS-Clean**, select **On**.

SIM Watch allows, if SIM card is replaced on the smartphone, to send to the specified number a new phone number and to block the stolen device. In order to use this function, select **On**.

If it is necessary to change the password used to work with Anti-Theft module, select the **Change password** item. Enter the new password and its confirmation and press the **OK** button.

Each time when you access the Anti-Theft module settings (see Figure 18) you have to enter the password you have set up earlier.



Figure 18. The **Anti-Theft** tab

Information about the module's work will be entered into the application log. In order to view the report, select the **Reports** item in the **Miscellaneous** tab.

2.2.7.6. SMS-Clean settings

To configure SMS-Clean settings, switch to the **Miscellaneous** tab and select the **Anti-Theft** item. Enter the password (see section 2.2.7.5 on page 24) and then select **SMS-Clean** in the window that will open.

Section **SMS-Clean** contains the list of data which can be selected for deletion if your smartphone gets stolen or lost (see Figure 19).

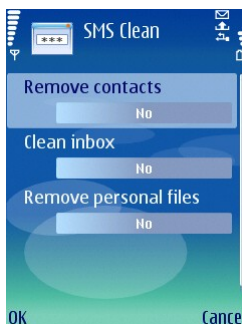


Figure 19. The **SMS-Clean** tab

If you wish to be able to delete the phone book once your mobile device has been stolen or lost, select the **Remove Contacts** item and assign value **Yes** to it.

In order to delete mail, SMS or MMS messages (Inbox and Mailbox folders) select the **Clean inbox** item and assign value **Yes** to it.

The **Remove personal files** item ensures deletion of personal data (data from folder `!\Data\`). By default deletion of personal files is not provided. If you wish to be able to delete your personal data in case your smartphone is stolen or lost, select this item and assign value **Yes** to it.

Press the **OK** button to save the changes you have made.

2.2.7.7. SIM Watch settings

To configure **SIM Watch** settings, switch to the **Miscellaneous** tab and select the **Anti-Theft** item. Enter the password (see section 2.2.7.5 on page 24) and then select **SIM Watch** in the window that will open.

Section **SIM Watch** is designed to monitor replacement of the SIM card in the device (see Figure 20).

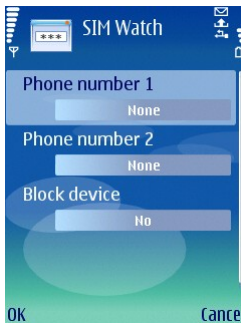


Figure 20. The **SIM Watch** tab

Using fields Phone number 1 and Phone number 2 enter phone numbers to which you would like to receive a new phone number if the SIM card was replaced in your smartphone. Such numbers may begin with a digit or with a "+" and must contain digits only.

Also you can configure blocking your smartphone if the SIM card was replaced. To do it, select the Block device item and assign value Yes to it. You can unblock the device by entering the password set up to access the Anti-Theft module. By default blocking of the device is not provided.

Press the **OK** button to save the changes you have made.

2.2.8. Updating the application bases

Scan for malware programs is performed based on the records in the application's bases which contain description of all malware programs known at the moment. It is extremely important to keep you bases up-to-date.

You can update bases manually or according to a schedule. Updates are performed from Kaspersky Lab's servers via internet.

You can enable automatic anti-virus scan of your smartphone after each update of the Kaspersky Mobile Security bases. In order to do it, switch to **Settings** item in the **Updater** tab and assign value **Enabled** to the **Scan on Update** item.

The value of the **Scan Quarantine on Update** setting determines whether or not objects in the quarantine will be rescanned each time after the application bases have been updated. By default the scan is performed. If you do not wish the scan to be performed, select **No**.

If you do not wish to select the internet access point each time you need to perform an update, select **No** as the value for the **Ask for Access Point** setting and the application will remember the last access point used when for the successful

update and will use this point to establish a network connection in the future. You can also configure a new access point.

If it is necessary to change the active access point, use the **Access point** setting. Then select the require value in the list. By default the access point is the default point of the device.

The value of the **Update server** setting determines the application bases update source: Kaspersky Lab's update servers (**Use default** value) or another server specified by the user (**User defined** value). If you selected the **Specify** value, enter the URL in the window that will open. If required, you can specify an alternative update server.

You can view detailed information about bases used in the **Database Info** item in the **Information** tab.

Information about bases update will be entered into the log. In order to view the log, select the **Reports** item in the **Updater** tab.

2.2.8.1. Configuring update settings

In order to configure application bases updates, perform the following actions:

1. Start Kaspersky Mobile Security (see section 2.2.2 on page 9).
2. Switch to the **Settings** item in the **Updater** tab (see Figure 21).

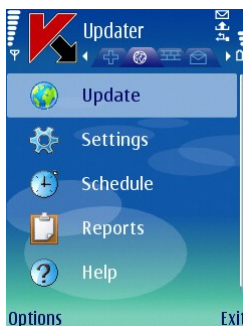


Figure 21. The **Updater** Tab

3. Enable / disable the prompt for the access point (the **Ask for Access Point** setting).

Note

The access point is configured using settings provided by your wireless service provider.

If you selected **No**, the connection will be provided using the access point used for the last update.

If the prompt option is enabled, you will be offered to select an access point from the list of available access points (see Figure 22).



Figure 22. Selecting the access point

4. Enter the address of the update server (if necessary). In order to do it, select the **Update server** item and then select the **User defined** value. Enter the URL of the update source in the window that will open (see Figure 23).

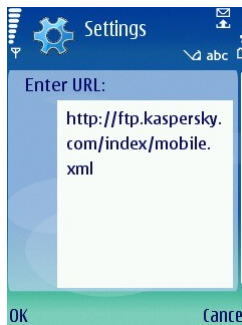


Figure 23. Update server address

By default updates are performed from Kaspersky Lab's update server: <http://ftp.kaspersky.com/index/mobile.xml>.

Warning!

Irrespective of whether the connection was opened earlier, it will be closed after the update is complete.

2.2.8.2. Manual update

In order to start an update manually,

1. Start Kaspersky Mobile Security (see section 2.2.2 on page 9).
2. Select the **Update** item in the **Updater** tab (see Figure 21).

2.2.8.3. Scheduled update

In order to configure scheduled bases update:

1. Start Kaspersky Mobile Security (see section 2.2.2 on page 9).
2. Select the **Schedule** item in the **Updater** tab and configure the **Automatic updates** settings:
 - **Off** – to not perform scheduled updates.
 - **Daily** - the update to be performed every day. Specify the update time in the corresponding field.
 - **Weekly** - the update will be performed once a week. Specify the update date and time in the corresponding fields.

2.2.9. Using the Firewall module

Firewall is designed for monitoring the network activity and protection of your smartphone at the network level (see Figure 24).

You can select the protection level (**Firewall** setting) in order to specify the level of control over the incoming and outgoing traffic out of the suggested options:

- **High** – all network activities are prohibited.
- **Medium** – all incoming connections are blocked, outgoing traffic of only regular applications is allowed.
- **Low** – only incoming connections are blocked.
- **Off** – all network activities are allowed.

Using the **Notification** setting you can configure receipt of notifications by the user if actions performed by the user do not correspond to the protection level selected. In order to disable receipt of notifications, select **Off**.



Figure 24. The **Firewall** tab

Information about the Firewall module's work will be entered into the application log. In order to view the report, select the **Reports** item in the **Firewall** tab.

2.2.10. Viewing report about the application operation

You can view the chronological event log about the operation of Kaspersky Mobile Security in the **Information** tab. In order to do it switch to this tab and select the **Reports** item (see Figure 25).



Figure 25. Report about the application's work

2.3. Removing the application

In order to remove Kaspersky Mobile Security from your smartphone, perform the following actions:

1. Close Kaspersky Mobile Security. To do it:
 - Press and hold the **Menu** button.
 - Select **KMS 7.0** in the list of the running applications and press the **Options** button.
 - Select the **Exit** menu item (see Figure 26).

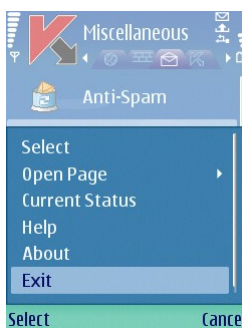


Figure 26. Closing the application

2. Remove Kaspersky Mobile Security
 - Press the **Menu** button and select the **Application Manager** menu item (see Figure 27).



Figure 27. Starting the Application Manager

- Select **KMS 7.0** in the list of applications and press the **Options** button (see Figure 28).



Figure 28. Selecting the application

- Select the **Remove** menu item (see Figure 29).

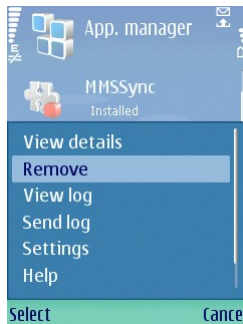


Figure 29. Removing the application

- Press the **Yes** button in the application removal confirmation window.

CHAPTER 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE

This chapter contains description of the operation of Kaspersky Mobile Security for mobile devices running one of the following operating systems:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

3.1. Installing Kaspersky Mobile Security

In order to install Kaspersky Mobile Security, perform the following steps:

1. Copy the cab archive with application installation package to your mobile device.
2. Run installation (open the cab archive with the distribution package on your mobile device). The application will be installed to the main memory of the mobile device.
3. Read the text of the license agreement. If you agree to all terms of the agreement, press **OK**. To cancel the installation, press **Cancel** (see Figure 30).

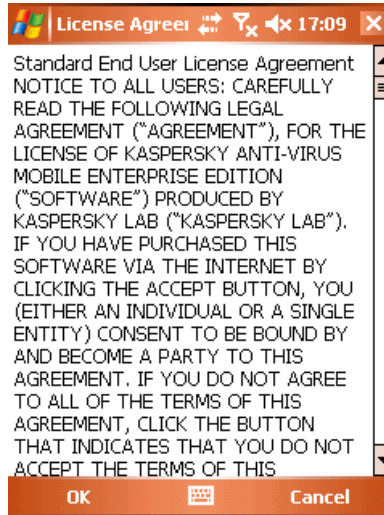


Figure 30. License Agreement

3.2. Getting started

This section contains information required to activate the application after it is installed to your mobile device and to start the application. It also contains information about the general principles of the graphic user's interface.

3.2.1. Activating the application

When you run the application for the first time, the Kaspersky Mobile Security activation window (see Figure 31) will be displayed on the mobile device's screen.

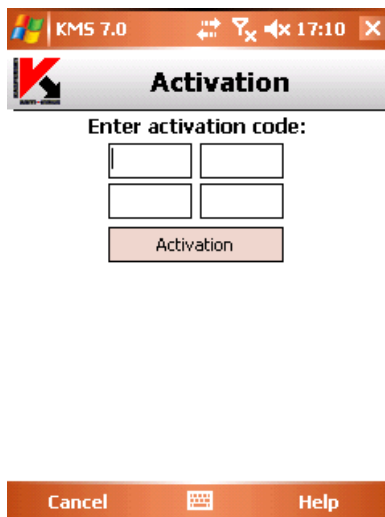


Figure 31. The Application activation window

Activation is necessary as without it all Kaspersky Mobile Security functions will not be available. You can receive the activation code at Kaspersky Lab's website.

Warning!

For the activation of Kaspersky Mobile Security you must have GPRS connection on your mobile device.

The activation code consists of Latin alphabet characters and digits (the code is case-insensitive). Enter the code into the four fields.

After you have entered the activation code, press **Activate**. The application will send an http query to Kaspersky Lab's activation server and will then download and install the license key.

If the activation code you entered appears invalid for any reason, a corresponding message will be displayed on your smartphone's screen.

3.2.2. Starting the application


In order to start Kaspersky Mobile Security, perform the following actions:

1. Open the **Programs** menu on your mobile device.
2. Select **KMS 7.0** in order to start the application.

After the application startup a window with main Kaspersky Mobile Security components (see Figure 32) will be displayed on your mobile device's screen.

- **Real-Time protection** – the use of the real-time protection mode.
- **Last Scanned** – date of the last anti-virus scan of your mobile device.
- **Last updated** – release date of Kaspersky Mobile Security database used by the application.

Warning!

If anti-virus scan of your mobile device has never been performed or if it two weeks or more have passed since the last update of the anti-virus database, the icon next to the corresponding item will look as follows: . This icon will also appear if the real-time protection mode or the Anti-Spam modules is disabled.

- **Firewall** – smartphone protection level.
- **Anti-Spam** – the status of the Anti-Spam module used for filtering SMS messages.

Warning!

Anti-Spam module is not provided for PDAs!



Figure 32. The Application component status window

3.2.3. Graphical user interface

The graphical user's interface consists of six tabs access to which is provided via **Menu** (see Figure 33):

- Using the **Scan** tab you can perform an anti-virus scan of the mobile device, edit the anti-virus scan and real-time protection mode and configure the auto scan schedule (see section 3.3 on page 38).
- Using the **Firewall** tab you can monitor the network activities and protect smartphone at the network level (see section 3.7 on page 52).
- Using the **Updater** tab you can update the anti-virus database, edit the updating settings and configure the updating schedule (see section 3.6 on page 50).
- Using the **Quarantine** tab you can manage the quarantine – a special-purpose storage for infected and suspicious objects (see section 3.4 on page 43).
- Using the **Other** tab you can configure filtering of incoming SMS and MMS messages (Anti-Spam module) and block the smartphone or erase information in case your device was stolen or lost (Anti-Theft module) (see section 3.5 on page 44).
- Using the **Information** tab you can view application component's operation logs, general information about the application and the anti-virus bases used and edit general settings used for application's operation (see section 3.8 on page 53).



Figure 33. 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**.

3.3. Anti-virus scan and protection

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

3.3.1. Real-time protection and on-demand scan

Real-time protection is the mode of operation in which the resident part of Kaspersky Mobile Security is constantly loaded in the mobile device's RAM and monitors all data in the device.

Real-time protection is started since the moment the device is turned on and works until it is turned off (if the use of this mode was not disabled by the settings).

Additionally, Kaspersky Mobile Security allows to perform a full scan of the mobile device's file system.

Information about the results of the real-time protection and of the on-demand scan will be recorded in the report. To view the report, select the **Scanner Report** item. The report can also be access via the **Information** tab (see section 3.8 on page 53).

In order to start the real-time protection use mode, perform the following:

1. Select the **Scanner Settings** item in the **Scan** tab.
2. Enable / disable the mode of using the real-time protection by checking/ unchecking the **Real-Time protection state** box.

In order to change the on-demand scan settings, perform the following:

1. Select the **Scanner Settings** item in the **Scan** tab.
2. Define the scan area in the **Scan options** block by selecting the file types to be scanned:
 - **Scan archives** - scan files packed into archives.
 - **Executables only** - scan only executable program files.
3. In the **If a virus is detected** block, determine the action to be performed by the application once an infected object is found. If you want Kaspersky Mobile Security to attempt to disinfect a detected infected object, check the **Try to disinfect** box. If disinfection is not required, select the possible anti-virus action by selecting one of the following values for the **Primary action** setting:
 - **Quarantine** – move infected objects detected to the quarantine.
 - **Ask User** - display a message about a virus detection on the screen with a suggestion to delete, quarantine or skip the infected object.
 - **Delete** - delete infected objects detected.
 - **Skip** – do not perform any action with the infected objects.

Additionally you can specify one of the actions for the case when the attempt to disinfect an infected object fails. In order to do this, check the **Try to disinfect** box and select the required action in the **If disinfection failed** list.

In order to start an anti-virus scan, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.2.1 on page 34).
2. Switch to the **Scanner Settings** tab.
 - Define the scan area in the **Scanner Settings** block by selecting the file types to be scanned (see above).
 - Determine the action to be performed by the application once an infected object is found (see above).
3. Using the **Scan** tab (see Figure 34) select the **Scan Phone** item if you wish to scan the entire file system of the mobile device or **Scan Folder** if you wish to scan an individual folder.

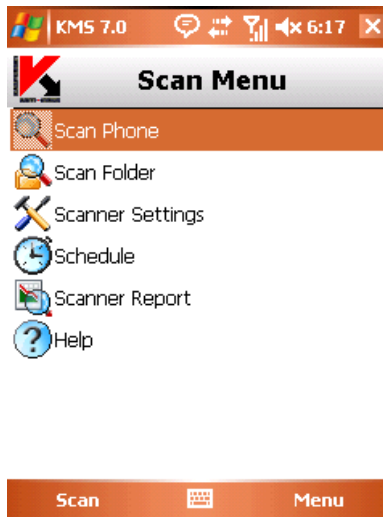


Figure 34. The **Scan** tab

If you selected the **Scan Folder** item, you will be transferred to the window displaying the mobile device's file system. In order to start the scan of a folder, move the cursor to the folder and press the **Scan** button.

After the scan is started, the scan process window will open in which the current status of the task will be displayed: the number of objects scanned and the path to the object currently being scanned (see Figure 35).

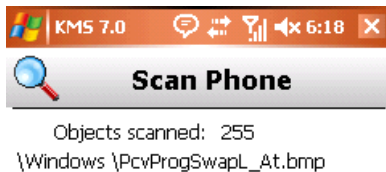


Figure 35. The Scan progress window

**Object:**

\\My Documents\\CORR-Eicar2.com

Infected with:

Eicar-test-file



Figure 36. Notification about virus detection

Once the scan is complete the general statistics about detected and deleted malware objects will be displayed.

3.3.2. Scheduled scan

Kaspersky Mobile Security allows the user to create the schedule for the automatic scan of the mobile device. The scan is performed in the background mode. When detecting an infected object an action specified in the scan settings will be performed with such object (the **Scanner settings** item).

By default scheduled scan is disabled.

In order to configure scheduled scan:

in the **Scan** tab select the **Schedule** item and configure the scan settings (see Figure 37):

- **Daily** - the scan to be performed every day. The scan time is determined by the **Time** setting.
- **Weekly** - the scan will be performed once a week. The date and time of the scan will be determined by settings **Week day** and **Time**.
- **Manual** - the update will be manually launched by the user.



Figure 37. The **Schedule** menu

3.4. Using Quarantine

Infected objects placed into the quarantine do not impose any threat for your mobile device and can be deleted or restored later.

Detected infected objects can be quarantined by the application automatically or after your confirmation.

In order to configure the application to automatically move infected objects found during the anti-virus scan to the quarantine, switch to the **Scan** tab, select the **Scanner settings** item and then select **Quarantine** as the value for the **Primary action** setting in the **If a is detected** block. For the case if the infected object could not be disinfected, check the **Try to disinfect** box and select **Quarantine** in the **If disinfection failed** list.

If you selected **Ask user** as the action to be performed, then, when an infected object is detected, Kaspersky Mobile Security will offer that you either delete this object or quarantine it.

In order view the quarantine contents switch to the **Quarantine** tab (see Figure 38).

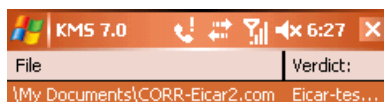


Figure 38. Quarantine

The **Menu** accessible from the quarantine view window allows the user:

- To view detailed information about the selected object in the quarantine (**Information** item).

- Delete the selected object (**Delete** item).
- Restore the current object from the Quarantine to its original folder (**Restore** item).
- Clear the quarantine by deleting all quarantined objects (**Delete all** item).

3.5. Using the Anti-Spam and the Anti-Theft modules

The Anti-Spam module is designed to ensure protection of your smartphone against unsolicited SMS and MMS messages.

Filtering is based on the use of "black" and "white" lists. Incoming messages received from phone numbers that had been added to the "black" list are blocked by Anti-Spam. Messages received from numbers that had been added to the "white" list, are not blocked.

The Anti-Theft is designed to ensure blocking the smartphone and erasing information stored in its memory in case it is lost or stolen.

3.5.1. Anti-Spam module

The Anti-Spam module is designed to ensure protection of your mobile against unsolicited SMS messages.

Filtering is based on the so-called "black" and "white" lists. Incoming messages received from phone numbers that had been added to the "black" list are blocked by Anti-Spam. Messages received from numbers that had been added to the "white" list, are not blocked.

In order to change the Anti-Spam work settings, perform the following:

1. Select **Settings** in the **Anti-Spam** tab.
2. Enable / disable the use of Anti-Spam by checking or unchecking the **Enable Anti-Spam** box.
3. Specify whether the receipt of SMS messages from phone numbers not found in either list is allowed, by checking or unchecking the **Receive SMS from: Unknown sender's** box.
4. Specify whether the receipt of SMS messages from phone numbers from the contact list is allowed by checking or unchecking the **Receive SMS from: People in my Contact List** box.

3.5.2. Editing “black” and “white” lists

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

The “White” list contains phone numbers from which the receipt of messages is allowed.

In order to edit the "black" or the "white" list, switch to the **Anti-Spam** tab (see Figure 39) and select the corresponding list.

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

- **Add entry** – add a new record to the list.
- **Delete entry** – delete record from the list.
- **Edit entry** – edit the current record in the list.

Select the **Add entry** item and specify your phone number (field **Enter number**) you wish to be included into the list. This number may begin with a digit or with a "+". Additionally when specifying a number, you can use masks "?" and "*".

You can also specify the text (**Enter text** field) upon the detection of which in a message the following actions will be performed:

- the message in which such text specified for the "white" list is found will be allowed to pass;
- the message in which such text specified for the "black" list is found will be blocked;

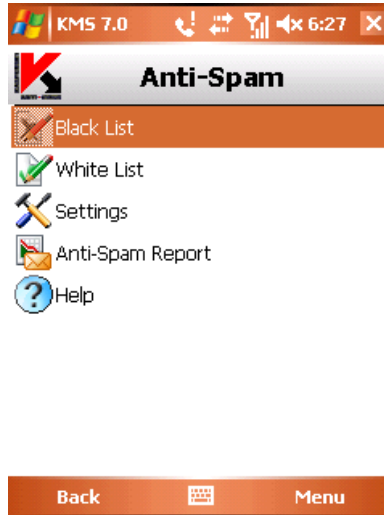


Figure 39. The **Anti-Spam** menu

Message analysis will be performed in the following order:

- check if the number is included into the "black" list;
- check if the number is included into the "white" list;
- check if the message text is included into the "black" list;
- check if the message text is included into the "white" list;

If the message meets any of these conditions, further analysis will not be performed and the message will be either allowed to pass or it will be blocked depending on whether it is included into the "black" or the "white" list.

After you have modified the list, press **OK** in order to return to the **Anti-Spam** tab.

3.5.3. Actions to be performed with messages

When you receive messages from a phone number not found in the "black" or "white" list depending that the Anti-Spam settings allow the receipt of message from unknown numbers (see section 3.5.1 on page 44), a warning will be displayed on the mobile device's screen (see Figure 40).

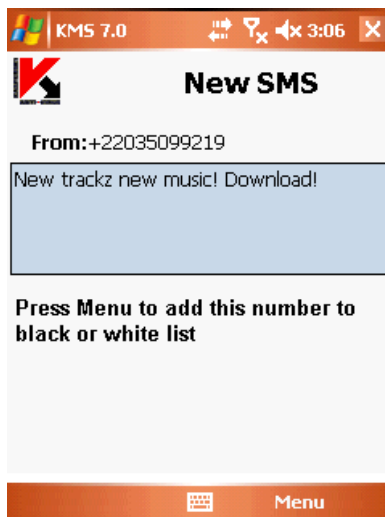


Figure 40. Anti-Spam warning

Using the **Menu** you can select one of the following actions to be performed with the message:

- **Add to "white" list** – allow receipt of messages and add the sender's phone number to the "white" list.
- **Add to "black" list** – block messages and add the sender's phone number to the "black" list.

Press the **Pass** button in order to let the message pass. In this case the sender's phone number will not be added to either of the lists.

Information about blocked messages will be entered into the application log. In order to view the log, press the **Report** button on the **Anti-Spam** tab or select the **Anti-Spam Report** item in this tab. The report can also be access via the **Information** tab (see section 3.8 on page 53).

3.5.4. The Anti-Theft module

This Anti-Theft module (the **Other** tab, item **Anti-Theft**) (see Figure 41) is designed to ensure protection of data stored on the mobile device against unauthorized access to it in case the device was list or stolen.

When you access the module settings for the first time you will have to set up a password. Using this password you can obtain access to the module's settings in order to modify them. The password is required in order to prevent unauthorized

access to the settings and to enable the user to block and erase information saved on the smartphone in case it is stolen or lost.

SMS-Block – allows blocking the device at the user's discretion. You can unblock the device only after you enter a password used to access the Anti-Theft module. This setting is enabled after the user of the stolen smartphone sends to this smartphone SMS: "*block:code*". The **SMS-Block** will be activate when it is selected: read the information message and press **OK** if you wish to use this function.

SMS-Clean allows erasing user's personal information (contact, incoming messages, personal files). This feature is triggered after the user of the stolen device sends to this device SMS: "*clean:code*". The **SMS-Clean** will be activated when it is selected: specify the required values for the settings (see section 3.5.4.1 on page 49), read the information message and press OK if you wish to use this function.

SIM Watch allows, if SIM card is replaced on the smartphone, to send to the specified number a new phone number and to block the stolen device. You can unblock the device by entering the password set up to access the Anti-Theft module. The **SIM Watch** will be activated when it is selected: specify the required values for the settings (see section 3.5.4.2 on page 50), read the information message and press OK if you wish to use this function.

If it is necessary to change the password used to work with Anti-Theft module, select the **Change password** item. Enter the new password and its confirmation and press the **OK** button.

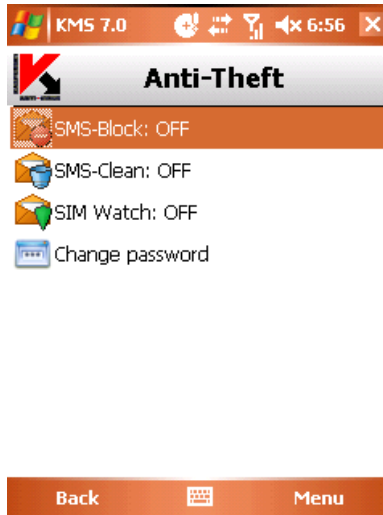


Figure 41. The **Anti-Theft** tab

Information about the Anti-Theft module's work will be entered into the application log. In order to view the log, select the **Anti-Theft Report** item in the **Other** tab. The report can also be accessed via the **Information** tab (see section 3.8 on page 53).

3.5.4.1. SMS-Clean settings

Section **SMS-Clean** contains the list of data which can be selected for deletion if your smartphone gets stolen or lost (see Figure 42).

In order to change the SMS-Clean function settings, perform the following:

1. Select **Anti-Theft** item on the **Other** tab.
2. Enter the password and select **SMS-Clean** in the window that will open.
3. Check the **contacts** box if you wish the phone book to be deleted once your mobile device has been stolen or lost.
4. Check the **inbox** if you wish to erase mail, SMS and MMS messages.
5. Check the **documents** box if you wish to erase user's personal data.
6. Check the **networks settings** box if you wish to erase networks settings.
7. Press **OK** to save the changes.

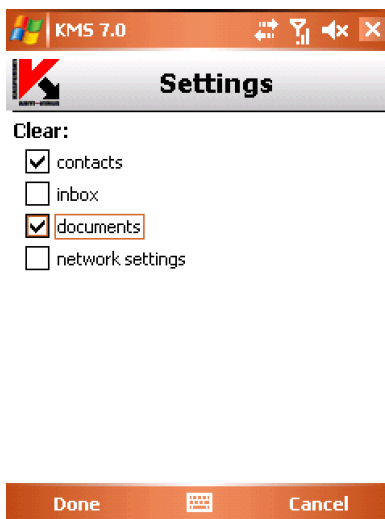


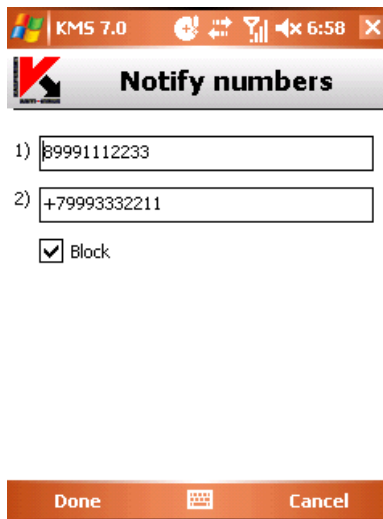
Figure 42. The **SMS-Clean** tab

3.5.4.2. SIM Watch settings

Section **SIM Watch** is designed to monitor replacement of the SIM card in the device (see Figure 43).

In order to change the SIM Watch function settings, perform the following:

1. Select **Anti-Theft** item on the **Other** tab.
2. Enter the password and select **SIM Watch** in the window that will open.
3. Using fields **1)** and **2)** enter phone numbers to which you would like to receive a new phone number if the SIM card was replaced in your smartphone. Such numbers may begin with a digit or with a "+" and must contain digits only.
4. Configure blocking of the mobile devices if the SIM card is replaced. In order to do it, check the **Block** box.
5. Press **OK** to save the changes you have entered.



The screenshot shows a dialog box titled "Notify numbers" from the KMS 7.0 application. The dialog has a title bar with the application name and system icons. Below the title bar, there is a logo and the title "Notify numbers". The main area contains two input fields labeled "1)" and "2)". The first field contains the number "89991112233" and the second field contains "+79993332211". Below these fields is a checkbox labeled "Block" which is checked. At the bottom of the dialog, there are two buttons: "Done" and "Cancel".

Figure 43. The **SIM Watch** tab

3.6. Updating the application bases

Scan for malware programs is performed based on the records in the Kaspersky Mobile Security bases which contain description of all malware programs known at the moment. It is extremely important to keep you bases up-to-date.

You can update bases manually or according to a schedule. To configure and start the update use the Update tab (see Figure 44). Updates are performed from Kaspersky Lab's servers via internet. In case an error occurs, make sure that the mobile device has access to the Internet.

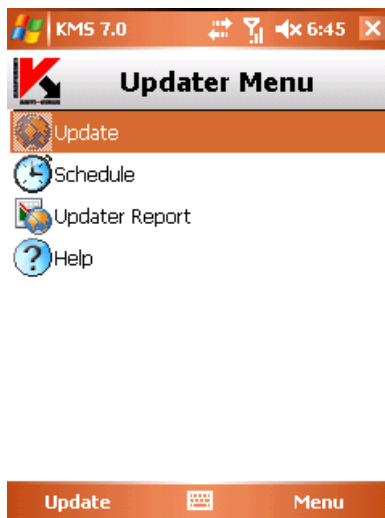


Figure 44. The **Update** Tab

Information about bases update will be entered into the log. In order to view the log, select the **Updater report** item in the **Updater Menu** tab. The report can also be access via the **Information** tab (see section 3.8 on page 53).

In order to manually launch the application bases update from Kaspersky Lab's update servers, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.2.1 on page 34) and switch to the **Update** tab.
2. Select **Update** in order to start downloading updates.

In order to configure the schedule for the automatic application bases update, perform the following:

1. Start Kaspersky Mobile Security (see section 3.2.1 on page 34) and switch to the **Update** tab.
2. In order to switch to editing of the automatic updating schedule settings, select **Schedule**.
3. Specify the updates frequency as the value for the update setting:

- **Daily** - the update to be performed every day. Additionally specify the **Time** of the update.
- **Weekly** - the update will be performed once a week. Additionally specify the **Week day** and the **Time** of the update.
- **Manual** - the update will be manually launched by the user.

In the **Information** tab you can view the release date of the anti-virus bases currently installed on your mobile device and the number of virus signatures. To do it, select the **Bases information** item in this tab.

3.7. Firewall

The **Firewall** module is designed for monitoring the network activity and protection of your mobile device at the network level (see Figure 45).

In order to change the firewall work settings, perform the following:

1. Start Kaspersky Mobile Security (see section 3.2.1 on page 34) and switch to the **Firewall** tab.
2. Select the **Firewall Settings** item. In the window that will open set the protection level to specify the level of monitoring of the incoming and outgoing traffic. You have following options:
 - **Block all** – all network activities are prohibited.
 - **Medium** – all incoming traffic is blocked, outgoing traffic of only regular applications is allowed.
 - **Low** – only incoming traffic is blocked.
 - **Disabled** – all network activities are allowed.

Information about the operation of the Firewall will be entered into the log. In order to view the log, select the **Firewall Report** item in the **Firewall** tab. The report can also be access via the **Information** tab (see section 3.8 on page 53).

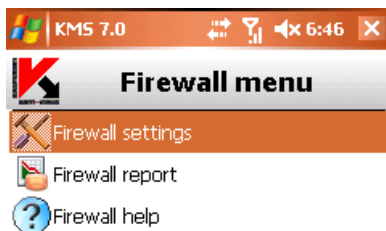


Figure 45. The **Firewall** tab

3.8. Viewing reports about the application operation

Reports about the application's work are located in the **Report** item of the **Information** tab. You can view a report on any task performed by Kaspersky Mobile Security:

- anti-virus scan;
- updating the application bases;
- firewall work;
- Anti-Spam module work;
- The Anti-Theft module work.

For example, in order to view an anti-virus scan report, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.2.1 on page 34).
2. Select the **Reports** item in the **Information** tab (see Figure 46).
3. Select a real-time protection report in the window that will open.

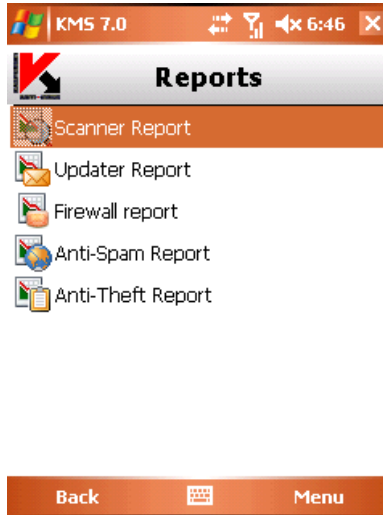


Figure 46. The **Reports** tab

3.9. Removing the application

In order to remove Kaspersky Mobile Security, perform the following actions:

1. Disable real-time protection (for more details see section 3.3 on page 38);

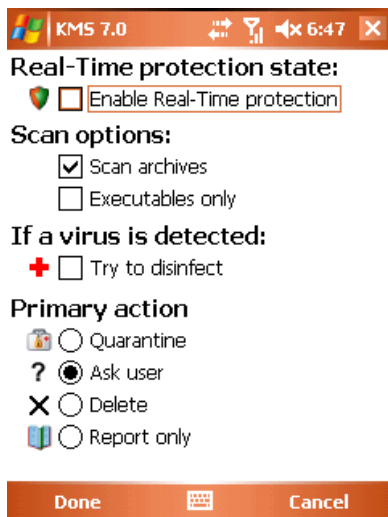


Figure 47. Closing real-time protection

2. Close Kaspersky Mobile Security. To do it select Exit in the application menu (see Figure 48).



Figure 48. Closing the application

3. Remove application. In order to do it:

- press the **Start** button, select the Settings button and then - **Remove applications** (see Figure 49):



Figure 49. Starting application removal

- Select **KMS 7.0** in the list of installed applications and press the **Remove** button (see Figure 50).

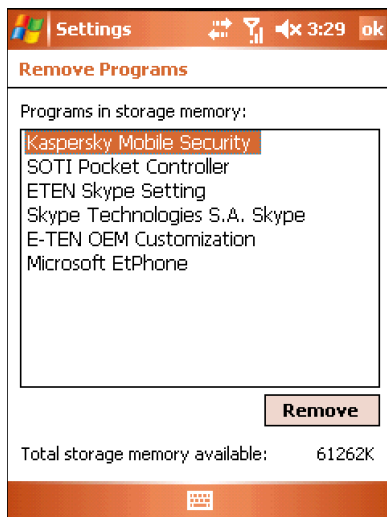


Figure 50. Selecting the application

- Press the **Yes** button in the application removal confirmation window (see Figure 51).

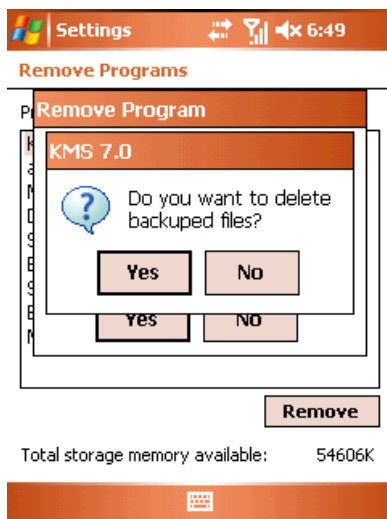


Figure 51. Prompt to confirm application removal

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 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 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.

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 ANTI-VIRUS (“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 Anti-Virus 7.0.

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 computer.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one computer 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 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/DVD-ROM, or other storage device) of that computer. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software’s proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

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

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

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

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

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

1.1.7 You shall not 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) Free software updates, including version upgrades;
- (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
- (d) Virus detection and disinfection updates in 24-hours period

(v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the

official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

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

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

5. *Limited Warranty.*

- (i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.
- (ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.
- (iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.
- (iv) 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).