Kaspersky Endpoint Security 8 for Smartphone

for Android™ OS

User Guide

PROGRAM VERSION: 8.0

Dear User!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers regarding this software product.

Note! This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation, and by international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by applicable law.

Reproduction or distribution of any materials in any format, including translations, is only allowed with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may be used exclusively for informational, non-commercial, and personal purposes.

Kaspersky Lab reserves the right to amend this document without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Kaspersky Lab shall not be liable for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential or actual losses associated with the use of these materials.

Document last revised on: February 8, 2012

http://www.kaspersky.com
http://support.kaspersky.com

TABLE OF CONTENTS

ABOUT THIS HELP

This document is the Guide for the installation, configuration and use of Endpoint Security 8 for Smartphone. The document is designed for a wide audience.

Objectives of the document:

- help the users independently set up the application on a mobile device, activate it and optimize the application for their needs;
- provide a rapid information search on issues connected with the application;
- give information on alternative sources of information about the application and possibilities of receiving technical support.

IN THIS SECTION

DOCUMENT CONVENTIONS

Conventions described in the table below, are used in this document.

Таблица 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted in red and enclosed in frames. Warnings contain important information, for example, on safety-critical computer operations.
It is recommended to use...	Notes are enclosed in frames. Notes contain additional and reference information.
Example: ...	Examples are given by section, on a yellow background, and under the heading "Example".
Update means...	New terms are marked by italics.
ALT+F4	Names of keyboard keys appear in a bold typeface and are capitalized. Names of the keys followed by a "plus" sign indicate the use of a key combination.
Enable	Names of interface elements, for example, input fields, menu commands, buttons, etc., are marked in a bold typeface.
➡ *To configure a task schedule:*	Instruction introductory phrases are marked in italics.
`help`	Texts in the command line or texts of messages displayed on the screen have a special font.
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of variables, the corresponding values are placed in each case (angle brackets are omitted).

ADDITIONAL DATA SOURCES

If you have questions about setting up or using Kaspersky Endpoint Security 8 for Smartphone, you can find answers from them, using various sources of information. You can choose the most suitable source according to how important or urgent your request is.

IN THIS SECTION

INFORMATION SOURCES FOR FURTHER RESEARCH

You can view the following sources of information about the application:

- the Kaspersky Lab application website;
- the application Knowledge Base page at the Technical Support Service website;
- the Help system;
- documentation.

Page on Kaspersky Lab website

http://www.kaspersky.com/endpoint-security-smartphone

Use this page to obtain general information about Kaspersky Endpoint Security 8 for Smartphone features and options.

The application page at the Technical Support Service website (Knowledge Base)

http://support.kaspersky.com/kes8m

This page contains articles written by experts from the Technical Support Service.

These articles contain useful information, recommendations, and the Frequently Asked Questions (FAQ) page, and cover purchasing, installing and using Kaspersky Endpoint Security 8 for Smartphone. They are arranged in topics, such as "Working with key files", "Database updates" and "Troubleshooting". The articles aim to answer questions about this Kaspersky Endpoint Security 8 for Smartphone, as well as other Kaspersky Lab products. They may also contain news from the Technical Support Service.

The Help system

If you have any questions about the Kaspersky Endpoint Security 8 for Smartphone separate screen or tab, you can view the context help.

To open the context help, open the right application screen and press **Help** or choose **Menu** → **Help**.

Documentation

The Kaspersky Endpoint Security 8 for Smartphone distribution kit includes the **User Guide** document (in PDF format). This document describes how to install and uninstall the application, manage its settings, start working with the application, configure the settings of its components. The document describes the application interface and the capabilities offered for typical application tasks.

DISCUSSION OF KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users in our forum at http://forum.kaspersky.com.

In the forum you can view existing discussions, leave your comments, and create new topics, or use the search engine for specific enquiries.

CONTACTING THE DOCUMENTATION DEVELOPMENT GROUP

If you have any questions about the documentation, or you have found an error in it, or would like to leave a comment, please contact our User documentation development group. To contact the Documentation Development Group send an email to docfeedback@kaspersky.com. Use the subject line: "Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Smartphone".

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone provides protection for mobile devices (herein "devices") running the Android™ operating system. The application can protect information on the device from infection by known threats, prevent unwanted SMS messages and calls, protect information on the device in case of theft or loss, and hide information relating to confidential contacts. Every type of threat is processed in separate components of the program. This allows to fine-tune the application settings depending on user needs.

Kaspersky Endpoint Security 8 for Smartphone includes the following protection components:

- **Anti-Virus** folder. It protects the file system of the mobile device from viruses and other malicious applications. Anti-Virus can detect and neutralize malicious objects on your device and update the application's anti-virus databases.

- **Anti-Spam** section. Scans all incoming SMS messages and calls for spam. The component allows the flexible blocking of text messages and calls considered undesirable.

- **Anti-Theft** folder. This protects information on the device from unauthorized access when it is lost or stolen and also makes it easier to find. Anti-Theft enables you to lock your device remotely, delete any information stored there, and pinpoint its geographic location using SMS commands from another device. Furthermore, Anti-Theft allows you to lock your device if the SIM card is replaced or if the device is activated without a SIM card.

- **Privacy Protection**. It hides information related to confidential numbers from the contact list. Privacy Protection hides entries in Contacts, call and SMS history, and incoming calls and SMS messages for these numbers.

Kaspersky Endpoint Security 8 for Smartphone does not back up and subsequently restore data.

IN THIS SECTION

HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Endpoint Security 8 can be installed on mobile devices running versions 1.6, 2.0, 2.1, 2.2, 2.3, 3.x, and 4.0 of the Android operating system.

INSTALLING KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

The administrator installs Kaspersky Endpoint Security 8 for Smartphone using remote administration tools. According to the user's means of administration, installation can be automatic or require further input from the user.

If the user's further input is needed to install the application, the installation will proceed in one of the following ways:

- The similar-named for installing the Kaspersky Endpoint Security 8 for Smartphone application installed on your computer. With this utility, you can install Kaspersky Endpoint Security 8 for Smartphone on your mobile device.
- You receive the email from the administrator with the distribution package or an indication to download it. You install Kaspersky Endpoint Security 8 for Smartphone on your mobile device using information from the email.

This section gives the preparatory actions for installing Kaspersky Endpoint Security 8 for Smartphone, it describes the different ways of installing applications on the mobile device and what the user has to do for each of them.

IN THIS SECTION

ABOUT INSTALLING THE APPLICATION VIA THE COMPUTER

If the administrator installed the Kaspersky Endpoint Security 8 for Smartphone supply utility on your computer, you can install Kaspersky Endpoint Security 8 for Smartphone to mobile devices connected to this computer. The Kaspersky Endpoint Security 8 for Smartphone supply utility contains the application distribution package and sends it to the mobile device. After it is installed on the workstation, the utility automatically launches and monitors the connection of mobile devices to the computer. Each time the mobile device connects to the workstation, the utility checks whether the device satisfies the requirements of Kaspersky Endpoint Security 8 for Smartphone, and offers to install the application on it.

INSTALLING THE APPLICATION VIA THE COMPUTER

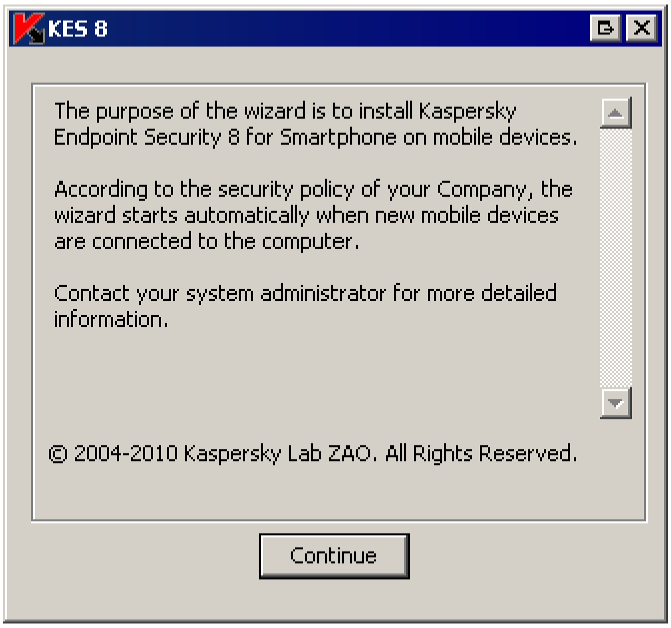
If the Kaspersky Endpoint Security 8 for Smartphone supply utility is installed on your computer, whenever mobile devices are connected that meet the system requirements you are prompted to install Kaspersky Endpoint Security 8 for Smartphone on them.

You can stop Kaspersky Endpoint Security 8 for Smartphone being installed on subsequent connections of the devices to the computer.

➧ *To install the application on a mobile device:*

1. Connect the mobile device to the computer.

   If the device meets the system requirements to install the application, the **KES 8** window opens with information on the utility (see figure below).



The purpose of the wizard is to install Kaspersky Endpoint Security 8 for Smartphone on mobile devices.

According to the security policy of your Company, the wizard starts automatically when new mobile devices are connected to the computer.

Contact your system administrator for more detailed information.

© 2004-2010 Kaspersky Lab ZAO. All Rights Reserved.

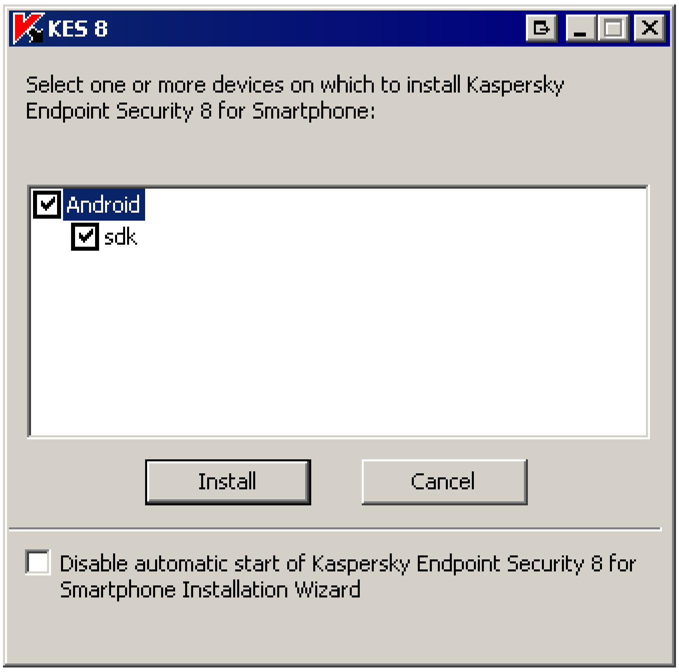
Figure 1. Kaspersky Endpoint Security 8 for Smartphone installation application

2. Press the **Continue** button.

   The **KES 8** window opens with a list of connected devices found.

   If more than one device which satisfies the system requirements is connected to the computer, they are shown in the **KES 8** window in the list of detected connected devices.

3. Select one or several devices from the list of detected connected devices on which the application needs to be installed. To do this, check the boxes next to the device names (see Figure below).



Select one or more devices on which to install Kaspersky Endpoint Security 8 for Smartphone:

☑ Android
  ☑ sdk

□ Disable automatic start of Kaspersky Endpoint Security 8 for Smartphone Installation Wizard

Figure 2. Selection of devices for installation of Kaspersky Endpoint Security 8 for Smartphone

4. Press **Install** button.

   The utility puts the distribution package on the selected devices. The **KES 8** window on the computer shows the status of the transfer of the distribution package.

   After the distribution package is transferred onto the chosen devices, application installation starts automatically.

Contact the administrator, if any errors occur during the installation process.

➧ *To prevent Kaspersky Endpoint Security 8 for Smartphone from installation to the connected devices,*

in the **KES 8** window check the **Disable automatic start of Kaspersky Endpoint Security 8 for Smartphone Installation Wizard** box.

ABOUT INSTALLING THE APPLICATION AFTER RECEIVING A EMAIL MESSAGE

You will receive an email message from the administrator with the distribution package or an indication to download it.

The message contains the following information:

- an attachment with the distribution package or a link to download it;
- information about the application connection settings to the remote administration system.

Save this message until Kaspersky Endpoint Security 8 for Smartphone is installed on the device.

INSTALLING THE APPLICATION AFTER RECEIVING EMAIL

➧ *To install Kaspersky Endpoint Security 8 for Smartphone:*

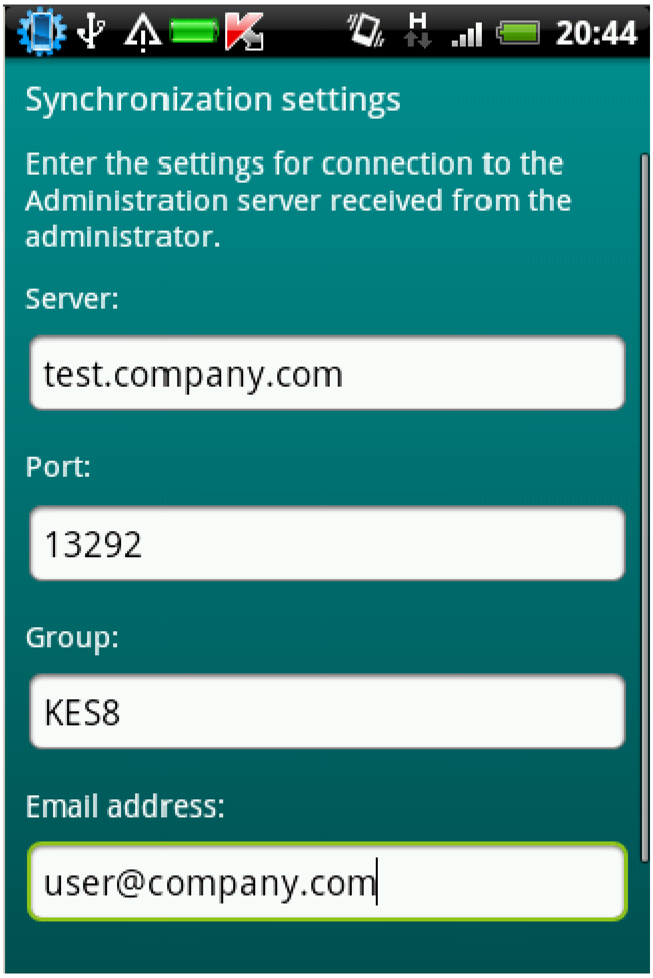
1. On the mobile device or the workstation, open the message from the administrator which contains the application installation settings.
2. Perform one of the following actions:
   - if the message has a link, follow it to download the distribution package;
   - if the distribution package is in an attachment to the message, download the distribution package.

   If you download the distribution package to a mobile device, it will be saved by default to the storage card.
3. Perform one of the following actions:
   - if you downloaded the distribution package to the mobile device, open it;
   - if you downloaded the distribution package to the workstation, connect the device to the workstation, copy the distribution package to the device, and open it.

     Installation starts automatically and the application will be installed on the device.

4. Run the application (see "Starting the application" on page 21). To do so, switch from the Home screen to the applications screen, and select Endpoint Security 8 for Smartphone.

   The **Synchronization settings** screen opens (see fig. below).



Synchronization settings

Enter the settings for connection to the Administration server received from the administrator.

Server:

test.company.com

Port:

13292

Group:

KES8

Email address:

user@company.com

Figure 3. Synchronization settings

5. Show the values for the settings to connect to the remote administration system if they were given when you received the message from the administrator. Enter the values for the following settings:

   - **Server**;
   - **Port**;
   - **Group**.

   If it is not necessary to configure the settings for connection to the remote administration system, this step will not be present.

6. In the **Your email address** field, enter your business email address and tap **Continue**.

   The email address is used for registering the device in the remote administration system. Please keep in mind that the email address specified during application installation cannot be changed.

7. Set the application secret code (see "Setting the secret code" on page. 21). To do this, you have to fill in the **Set secret code** and **Confirm code** fields and tap **Enter**.

8. Enable the option to recover the secret code (see "Enabling the option to recover the secret code" on page 22).

Contact the administrator, if any errors occur during the installation process.

UNINSTALLING THE APPLICATION

The application can only be uninstalled from the device if hiding of confidential information is disabled. Before uninstalling the application, you should ensure that this condition is fulfilled.

➡ *To uninstall Kaspersky Endpoint Security 8 for Smartphone:*

1. Disable Privacy Protection (on page 61).
2. From the Home screen go to the applications screen and select **Settings** → **Applications** → **Manage applications**.
3. Select Kaspersky Endpoint Security 8 for Smartphone from the list of applications.

   The **About the application** screen opens.
4. Tap the **Delete** button.

   A confirm deletion window opens.
5. Confirm the deletion of Kaspersky Endpoint Security 8 for Smartphone by tapping **OK**.

   The application is deleted from the device.
6. Tap the **ОК** button when deletion is complete.

MANAGING APPLICATION SETTINGS

All Kaspersky Endpoint Security 8 for Smartphone settings including the license are configured by the administrator through the remote administration system. The administrator can set the user permission to change the values of these settings.

You can change the application settings on your mobile device if the administrator has not disabled the capability to change these parameters.

The administrator can block changing all or some components. If the component settings screen has a lock icon and a warning message, the settings of the component cannot be accessed to be changed on the mobile device.

If the administrator changed the application settings, they are transferred to the device via the remote administration system. In this case the values of the application settings blocked by the administrator will change. Settings that were not blocked by the administrator will remain unchanged.

If the application settings were not transferred to the device, or you want to restore the values set by the administrator, use the function to synchronize the device with the remote administration system (see "Synchronizing with the remote administration system" on page 18).

Only use the synchronization function under the administrator's guidance.

MANAGING THE LICENSE

This section gives information about the application license, how to activate it and view information about it.

IN THIS SECTION

ABOUT KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE LICENSES

A *license* is the right to use Kaspersky Endpoint Security 8 for Smartphone and the additional services associated with it as provided by Kaspersky Lab or its partners.

The license must be installed to be able to use the application.

Every license has a validity period and type.

License term – a period during which the additional services are offered:

- technical support;
- update the application's anti-virus databases.

The scope of services provided depends on the license type.

The following license types are available:

- *Trial* – a free license with a limited validity period, e.g. 30 days, offered to allow you to get acquainted with Kaspersky Endpoint Security 8 for Smartphone.

  During the trial license period of validity, all application functions are accessible. Upon expiration of its validity period, Kaspersky Endpoint Security 8 for Smartphone stops performing all of its functions. When this happens, only the following actions are available:

  - disabling hiding of personal data;
  - viewing the application's help system;
  - synchronizing with the remote administration system.

- *Commercial* – paid license with a limited validity period (for example, one year), provided upon purchase of Kaspersky Endpoint Security 8 for Smartphone.

  If a commercial license is activated, all application features and additional services are available.

  On termination of its commercial license's validity, Kaspersky Endpoint Security 8 for Smartphone limits the application's functionality. You can continue to use the Anti-Spam component, perform an anti-virus scan of the mobile device and use protection components, but only on the basis of anti-virus databases that are current on the date of the license expiry. For other application components, only the following actions are available:

- disabling hiding of personal data;
- viewing the application's help system;
- synchronizing with the remote administration system.

INSTALLING A LICENSE

The administrator installs the license through the remote administration system.

Kaspersky Endpoint Security 8 for Smartphone works without a license with full functionality for three days after it is installed. During this time, the administrator installs the license through the remote administration system and the application is activated.

If the license was not installed during the three days, the application works in a limited function mode. The following are accessible in this mode:

- start virus scan;
- configure additional application settings;
- start synchronization of the device with the remote administration system;
- disabling hiding of personal data;
- viewing application help system.

If the license was not installed within three days of installation, use the function to synchronize the device with the remote administration system to install the license.

VIEWING LICENSE INFORMATION

You can view the following license information: license number, type, activation date, expiration date, number of days to expiration and device serial number.

➡ *To view the license information:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

   This will open the **Additional** window.

2. Select the **License** item.

SYNCHRONIZATION WITH THE REMOTE ADMINISTRATION SYSTEM

During synchronization, the application settings configured by the administrator are transferred to the device. Operational reports on the application components are transferred from the device to the remote administration system.

The device is automatically synchronized with the remote administration system.

If synchronization does not perform automatically, you can start it manually.

Manual synchronization is required, if the license was not installed within three days after application installation.

According to the remote administration system chosen by the administrator to manage the application, the user may be asked to enter connection settings to the remote administration system. In this case, the values set by the user manually are accessible for changes in the application (see "Changing the synchronization settings" on page 20).

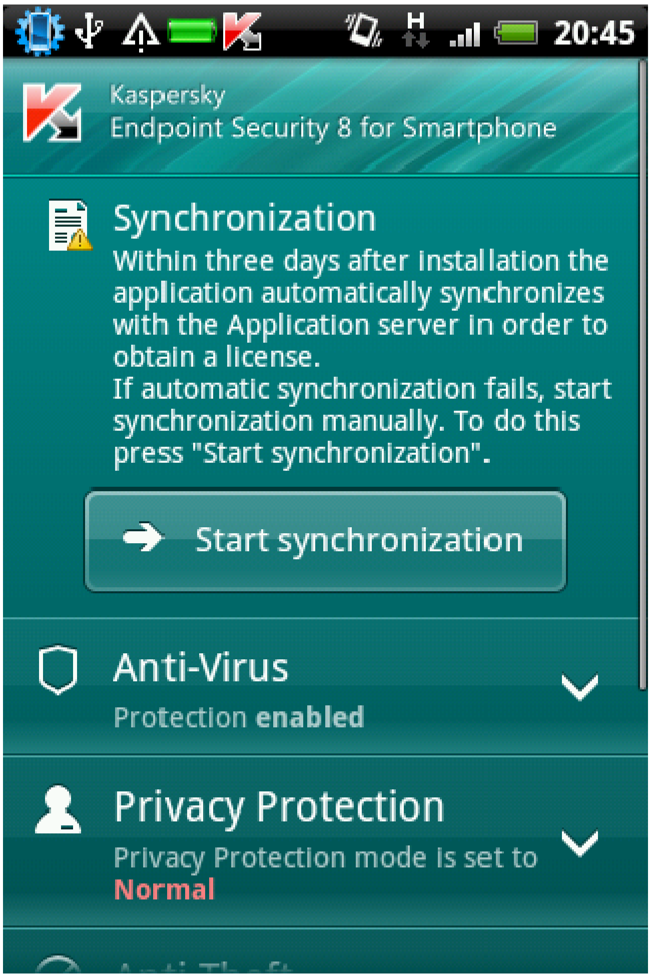
Change the settings for connection to the remote administration system only under the administrator's guidance.

IN THIS SECTION

START SYNCHRONIZATION MANUALLY

➡ *To manually synchronize the device with the remote administration system after the application is installed,*

after the warning on the Home screen tap **Start synchronization** (see Figure below).



20:45

Kaspersky
Endpoint Security 8 for Smartphone

Synchronization

Within three days after installation the application automatically synchronizes with the Application server in order to obtain a license.
If automatic synchronization fails, start synchronization manually. To do this press "Start synchronization".

Figure 4. Starting synchronization

The option to start synchronization on the Home screen of Kaspersky Endpoint Security 8 for Smartphone after the application is installed is available if automatic connection to the remote administration system failed.

When synchronization is complete, the application settings are applied on the device, the license is installed, and the **Start synchronization** button is not displayed on the Home screen.

➡ *To manually synchronize the device with the remote administration system:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

   This will open the **Additional** window.

2. Tap **Synchronize**.

   If the user was not prompted to enter settings to connect to the remote administration system during installation, a connection is established with the remote administration system.

   If the user was prompted to enter settings to connect to the remote administration system during installation, the menu item is called **Synchronization** and the **Synchronization** screen opens. Tap **Synchronize**. Internet connection with the remote administration system will be set.

CHANGING THE SYNCHRONIZATION SETTINGS

Change the settings of connection to the remote administration system only if directed by the administrator.

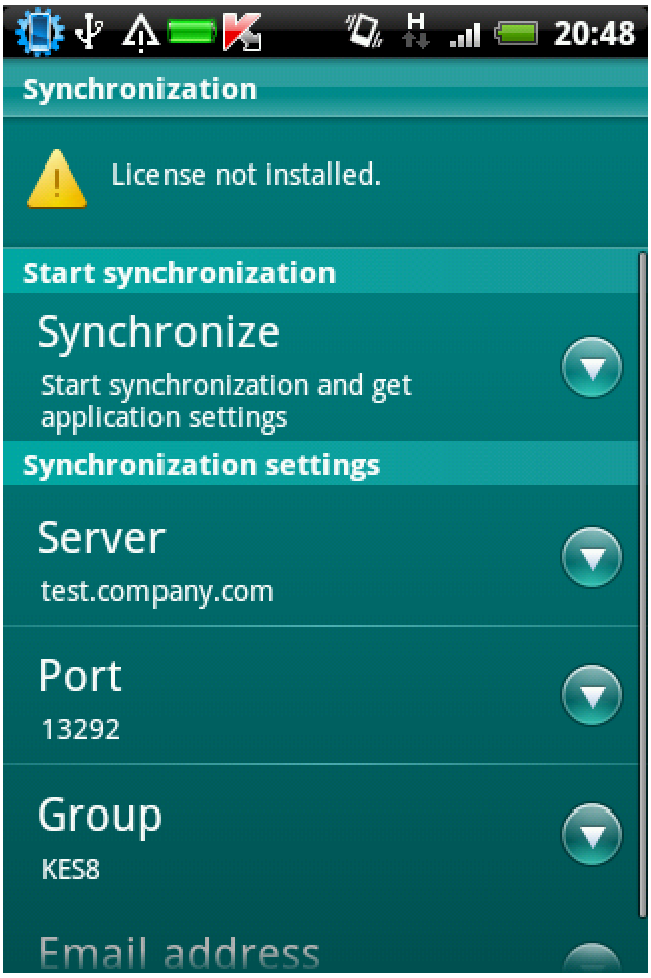
➡ *To change settings for connection to the remote administration:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.

   This will open the **Additional** window.

2. Select **Synchronization**.

   The **Synchronization** screen opens (see figure below).



20:48

Synchronization

License not installed.

Start synchronization

Synchronize

Start synchronization and get application settings

Synchronization settings

Server

test.company.com

Port

13292

Group

KES8

Email address

Figure 5. Synchronization settings

3. Change the values of the following settings in the **Synchronization settings** section:

   - **Server**;
   - **Port**;
   - **Group**.

GETTING STARTED

This section provides information about how to start using Kaspersky Endpoint Security 8 for Smartphone: activate it, set a secret code for the application, enable the option of secret code recovery, recover the secret code, and start the application.

IN THIS SECTION

STARTING THE APPLICATION

➧ *To start Kaspersky Endpoint Security 8 for Smartphone:*

1. Switch from the Home screen to the applications screen.
2. Select **Kaspersky Endpoint Security 8 for Smartphone**.
3. Enter the secret code of the application and tap **Enter**.

The Home screen opens.

SETTING THE SECRET CODE

After starting the application you will be asked to enter the application secret code. *Application secret code* prevents any unauthorized access to the application settings.

You can later change the secret code installed.

Kaspersky Endpoint Security 8 for Smartphone prompts for the secret code in the following cases:

- for access to the application;
- when sending an SMS command from another mobile device to start the following functions remotely: Block, Data Wipe, SIM Watch, GPS Find, Privacy Protection.

The secret code is comprised of numerals. The minimum number of characters is four.

If you forget the application secret code, you can restore it (see the "Recovering the secret code" section on page 23). For this purpose, the recovery of secret code option must be enabled in advance (see the "Recovering the secret code" section on page 23).

➡ *To enter the secret code:*

1. After activating the application, enter in the **Enter secret code** field the figures which will be your code.

   The code entered is automatically verified.

   If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. In order to use the code, press **Yes**. In order to create a new code, press **No**. Enter a new application secret code.

2. Re-enter the same code in the **Confirm new code** field.

   The secret code is now set.

ENABLING THE OPTION TO RECOVER THE SECRET CODE

After the initial activation of the application, you can enable the option of secret code recovery. Then, in the future, you will be able to recover the secret code if it is forgotten.

If you have canceled the option enabling during the initial activation of the application, you can enable it after reinstallation of Kaspersky endpoint Security 8 for Smartphone on the device.

You can only recover the application secret code (see the "Recovering the secret code" section on page 23) if the recovery of secret code option is enabled. If you forget the password, and the recovery of secret code option is disabled, it will not be possible to manage the functions of Kaspersky Endpoint Security 8 for Smartphone.

➡ *To enable the recovery of secret code option:*

1. After you have installed the secret code for the application (see the "Setting the secret code" section on page 21) enter your email address on the **Enabling the option to recover the secret code** screen.

2. Confirm the enabling of the option of secret code recovery, by tapping **Enable**.

   The email address that you give will be used during recovery of the secret code.

   The application will establish an Internet connection with the secret code recovery server, send the information entered and enable the recovery of secret code option.

Recovering the secret code

You can only recover the secret code enabling the recovery of secret code option in advance (see "Enabling the option to recover the secret code" on page 22).

➧ *To recover the application secret code:*

1. Switch from the Home screen to the applications screen.
2. Select **Kaspersky Endpoint Security 8 for Smartphone**.
3. Tap **Menu** → **Recovery of secret code**.

   The following information will then be displayed on the screen:

   - Kaspersky Lab's website to recover the secret code;
   - device identification code.
4. Tap **Go**.

   The website for your secret code recovery http://mobile.kaspersky.com/recover-code opens.
5. Enter the following information in the appropriate fields:

   - the email address that you previously designated for recovery of the secret code;
   - device identification code.

   As a result, the recovery code will be sent to the email address that you indicated.
6. Switch to the **Kaspersky Endpoint Security 8** screen.
7. Tap **Menu** → **Enter recovery code** and enter the recovery code that you received.
8. Enter the new application secret code. To do so, enter the new secret code in the **Set new secret code** and **Confirm new secret code** fields.
9. Tap **Enter**.

Viewing information about the application

You can view general information about Kaspersky Endpoint Security 8 for Smartphone and its version.

➧ *To view information about the application:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

   This will open the **Additional** window.
2. In the **Information** section, select the **About the application** item.

APPLICATION INTERFACE

This section provides information on the basic elements of Kaspersky Endpoint Security 8 for Smartphone interface.

IN THIS SECTION

HOME SCREEN

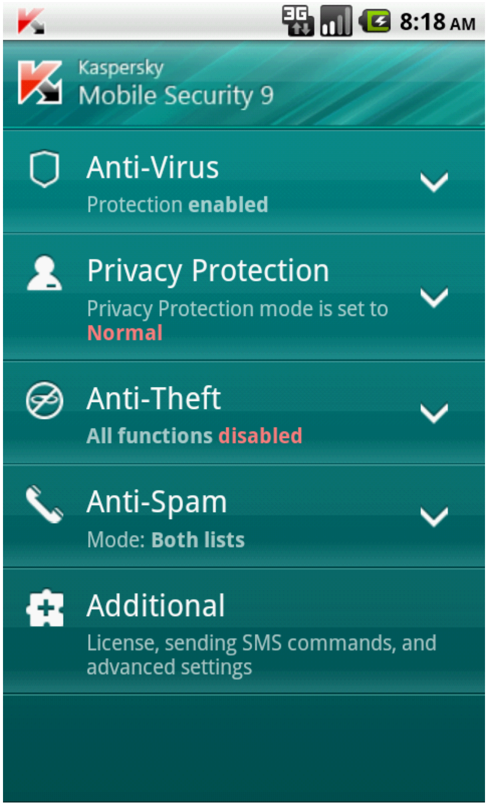
When the application starts, the Home screen opens (see fig. below).

Dropdown sections are located on the Home screen. Each section can be used to configure a component or run protection tasks.

The Home screen also displays the status of the main components.

The following information is shown under the name of each section:

- **Anti-Virus** – protection status of the device against viruses and other threats (see "File system protection" on page 26).
- **Privacy Protection** – mode for hiding confidential information.
- **Anti-Theft** – status of the Anti-Theft functions.
- **Anti-Spam** – mode for filtering calls and SMS messages.
- **Additional** – information about additional application settings grouped in this section (see "Configuring additional settings" on page 71).



Anti-Virus
Protection **enabled**

Privacy Protection
Privacy Protection mode is set to **Normal**

Anti-Theft
All functions disabled

Anti-Spam
Mode: **Both lists**

Additional
License, sending SMS commands, and advanced settings

Figure 6. Home screen

HOME SCREEN WIDGET

The Home screen of Kaspersky Endpoint Security 8 includes a widget (see fig. below).

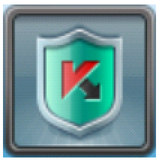


Figure 7. Home screen widget

The color indicator of the Home screen widget informs you about the protection status of your device, Privacy Protection and the license, and allows you to configure the application settings.

The color scheme is used:

- a green shield indicates that Protection is enabled;
- a grey shield indicates that Protection is disabled;
- a green background indicates the confidential information is hidden;
- a grey background indicates that confidential information is displayed;
- an exclamation mark in a yellow triangle indicates that the license has expired or it is not installed.

FILE SYSTEM PROTECTION

This section provides information on the Protection component which enables avoidance of infections of your device's file system. The section also describes how to activate/stop the Protection and adjust its operation settings.

IN THIS SECTION

ABOUT PROTECTION

Protection starts when operation system starts up and is always found in the device's memory. Protection scans all files that can be opened, saved or executed (including ones located on storage cards), and installed applications.

File scanning is performed as follows:

1. Protection scans every file when the user accesses it.

   Protection analyses the file for the presence of malicious objects. Malicious objects are detected by comparison with the application's anti-virus databases. The anti-virus databases contain descriptions of all currently known malicious objects, and methods for neutralizing them.

2. According to the file analysis results, the following types of Protection behavior are possible:

   - If malicious code is detected in a file, Protection performs an action in accordance with the settings (see "Selecting an action to be performed on detected objects" on page 29);

   - If no malicious code is discovered in the file, it will be immediately made accessible.

Protection scans the installed application for viruses when it is first started. Protection performs the scan on the basis of the anti-virus databases. If Protection detects a virus during the scan, it prompts the user to delete the application.

Application scanning is performed as follows:

1. Protection scans the installed application for malicious objects when it is first started.

   Protection uses the anti-virus database to perform the scanning procedure according to the selected mode.

2. Based on the scan results, Protection may take the following steps:

   - If malicious code is revealed during application scanning, Protection will suggest removing that application.

   - If no malicious code is found during application scan, the application becomes available.

ENABLING / DISABLING PROTECTION

When activating the Protection, all actions in the system are under permanent control.

Device resources are expended to ensure protection against viruses and other threats. In order to reduce the load on the device when executing several tasks, you can temporarily stop Protection.

> Kaspersky Lab recommends you not to disable real-time protection because it may lead to your device becoming infected with viruses, with possible data loss.

Disabling Protection does not affect running virus scan tasks and updating application anti-virus databases.

The current status of Protection is displayed on the Home screen in the **Anti-Virus** section.

➡ *To enable Protection:*

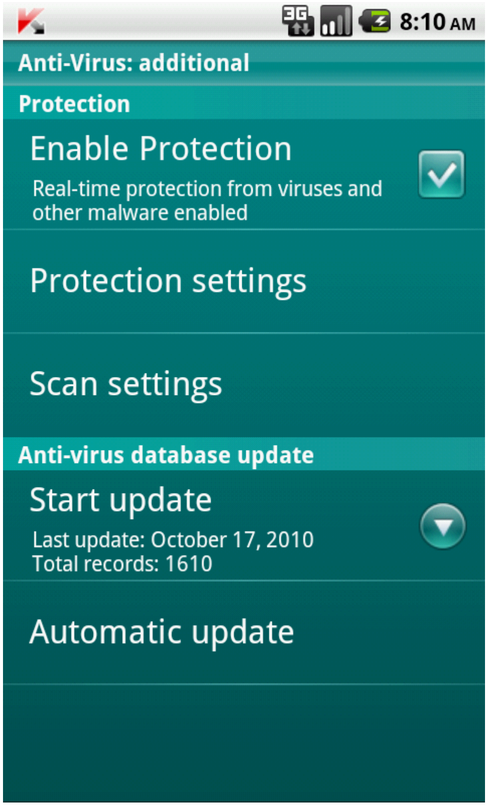
1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** folder.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Check the **Enable Protection** box (see Figure below).

➡ *To disable Protection:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** folder.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Uncheck the **Enable Protection** box.



8:10 AM

Anti-Virus: additional

Protection

Enable Protection ☑
Real-time protection from viruses and other malware enabled

Protection settings

Scan settings

Anti-virus database update

Start update
Last update: October 17, 2010
Total records: 1610

Automatic update

Figure 8. Enabling Protection

CONFIGURING THE PROTECTION AREA

By default Kaspersky Endpoint Security 8 for Smartphone scans all file types. You can select file types for Kaspersky Endpoint Security 8 for Smartphone to check for the presence of malicious objects during Protection operation.

Before you configure the Protection settings, make sure that **Maximum** Protection mode is enabled.

➡ *To select the type of files to be scanned:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** folder.

2. Tap **Additional**.

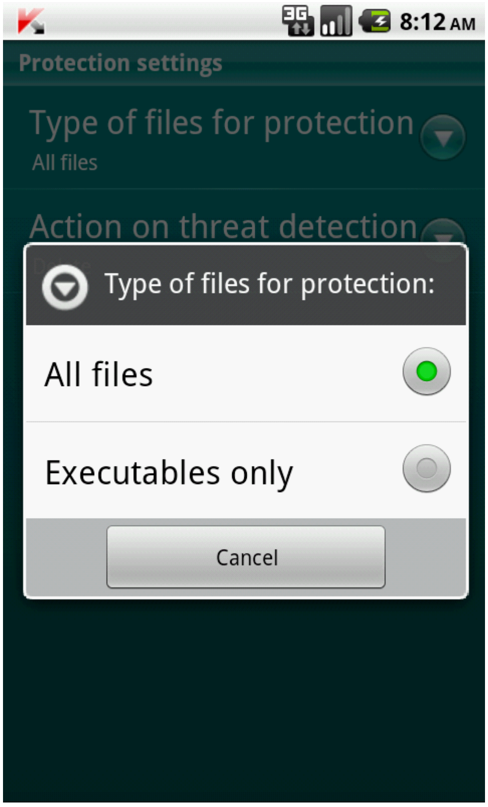
   The **Anti-Virus: Additional** screen opens.

3. Select **Protection settings** → **Type of protected files**.

4. Select a value for the **Type of protected files** setting (see fig. below):

   - **All files**: scan all types of files.

   - **Executables only** – scan executable files of applications only (for instance, files of the formats EXE, MDL, APP, DLL files).



Protection settings

Type of files for protection
All files

Action on threat detection

Type of files for protection:

All files ●

Executables only ○

Figure 9. Selecting the objects to scan

SELECTING THE ACTION TO BE PERFORMED ON DETECTED OBJECTS

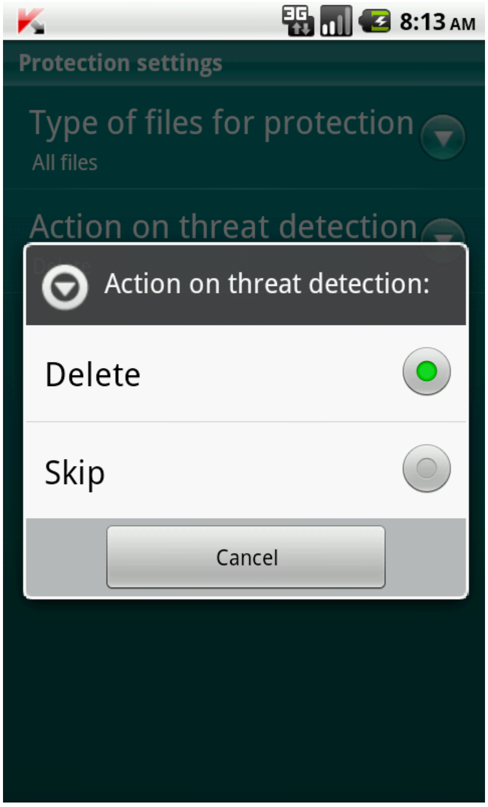
By default, Kaspersky Endpoint Security 8 for Smartphone deletes the detected threat. You can choose the activity which Kaspersky Endpoint Security 8 for Smartphone fulfills on the detected malicious threat.

Before you configure the Protection settings, make sure that **Maximum** Protection mode is enabled.

➡ *To configure the application response on detection of a threat:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** folder.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Select **Protection settings** → **Action when threat is detected**.
4. Set the action that the application takes if it detects a threat. To do so, select a value for the **Action when threat is detected** setting (see fig. below):
   - **Delete**: delete malware objects without notifying the user.
   - **Skip** – skip malicious objects without deleting them from the device.



Protection settings

Type of files for protection
All files

Action on threat detection

Action on threat detection:

Delete ●

Skip ○

Figure 10. Selecting an action to perform when a threat is detected

SCANNING THE DEVICE

This section gives information about scanning the device on demand, which can detect and remove threats on your device. The section also describes how to launch a scan of the device, set up an automatic scheduled file system scan, select files for scanning, and set the action that the application will take when a malicious object is detected.

IN THIS SECTION

ABOUT SCANNING THE DEVICE

Scanning the device on demand helps to detect and neutralize malicious objects. Kaspersky Endpoint Security 8 for Smartphone can perform either a full scan of the device content or a partial scan – i.e. scan only the content of the device's built-in memory or a specific folder (including those located on the storage card).

The device is scanned as follows:

1. Kaspersky Endpoint Security 8 for Smartphone scans files of the selected type (see "Selecting an object type to be scanned" on page 33).

2. During the scan, each file is analyzed for the presence of malicious objects (malware). Malicious objects are detected by comparison with the application's anti-virus databases. Anti-Virus databases contain descriptions of all known malicious objects, and methods for neutralizing them.

   If no malicious code is detected, the file immediately becomes accessible for operation.

   If the application detects malicious code in a file, it performs the action selected in accordance with the settings (see "Selecting an action to be performed on detected objects" on page 34).

The scan starts manually or automatically in accordance with a schedule (see "Starting a scheduled scan" on page 32).

STARTING A SCAN MANUALLY

You can manually start a full or partial scan as required.

➧ *To start an anti-virus scan manually:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.

2. Select **Start scan**.

3. Select the device scan area (see Figure below).

   - **Full scan** – scan the device's entire file system. By default, the application scans files saved to the device's onboard memory and memory cards.

   - **Folder scan** – scan a separate object in the device file system or on the storage card. When **Folder scan** is selected, the **Folder selection** screen displaying the device file system opens. To start a folder scan, select the required folder and tap the scan icon located to the right of the name of the folder.

   - **Memory scan**: scan the processes started in the system memory and its corresponding files.

After the scan begins, a scan progress window opens showing the current task status: the number of files scanned, the path to the file currently being scanned, and an indication of the scan results as a percentage. In the scan progress window, you can pause the scan by tapping **Pause**, or cancel the scan by tapping **Cancel**.

If Kaspersky Endpoint Security 8 for Smartphone detects a malicious object, it performs an action in accordance with the scan parameters set (see the "Selecting an action to be performed on detected objects" section on page 34).

By default, if Kaspersky Endpoint Security 8 for Smartphone finds a malicious object, it attempts to disinfect it. If disinfection is not possible, the application deletes the malicious object.

When the scan is completed, overall statistics are displayed on the screen with the following information:

- number of scanned files;
- number of viruses detected and deleted;
- number of files passed through (for instance, a file is blocked by the operating system or a file is not executable, when scanning only executable program files);
- scan time.

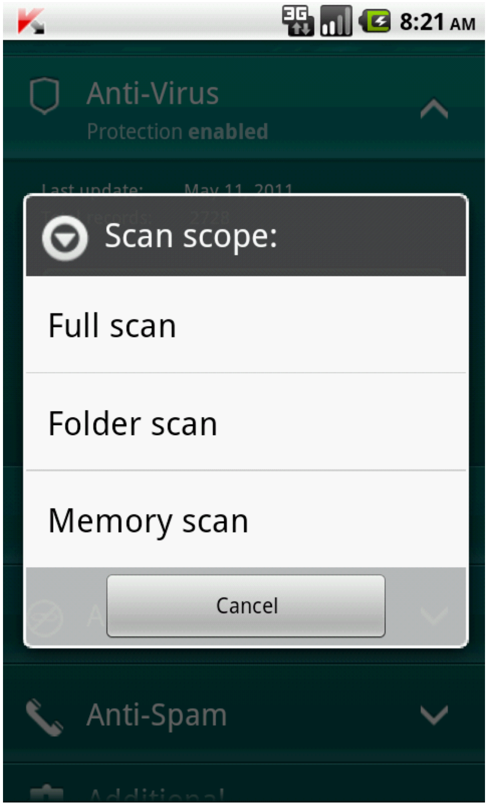


Figure 11. Selecting the scan area

STARTING A SCHEDULED SCAN

You can configure automatic startup of the file system scan upon a schedule. A scheduled scan is carried out in background mode. When a malicious object is detected, the action selected in the scan settings will be performed on it (see "Selecting an action to be performed on detected objects" section on page 34).

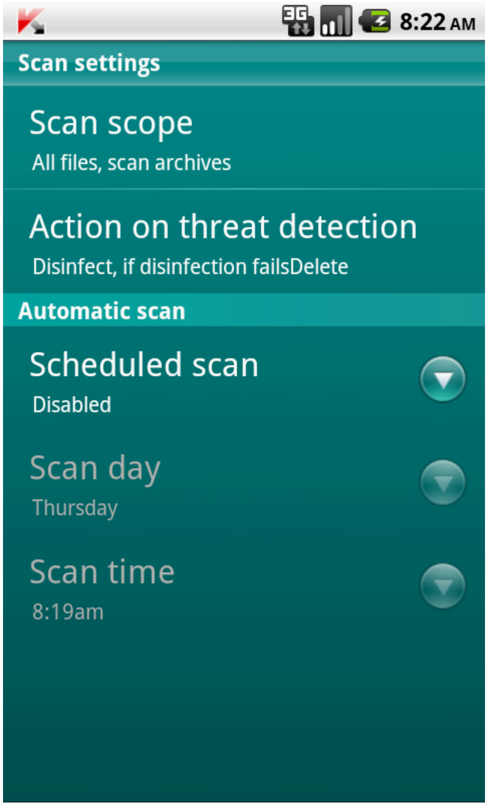
By default, starting a scheduled file system scan is disabled.

➡ *To set a scan schedule:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Select **Scan settings**.

   The **Scan settings** screen opens.
4. Select the start scan mode. To do so, assign a value to the **Scheduled scan** (see fig. below) setting:
   - **Weekly** – perform the scan once a week. For this mode, set the day and time of the scan. Select values for the settings **Scan day** and **Scan time**.
   - **Daily** – perform the scan every day. For this mode, set the time of the scan. Select a value for the **Scan time** setting.
   - **Disabled** – disable scheduled scans.



Scan settings

Scan scope
All files, scan archives

Action on threat detection
Disinfect, if disinfection failsDelete

Automatic scan

Scheduled scan
Disabled

Scan day
Thursday

Scan time
8:19am

Figure 12. Configuring an automatic scan schedule

SELECTION OF OBJECT TYPE TO BE SCANNED

By default, Kaspersky Endpoint Security 8 for Smartphone scans all files stored on the device and storage card. To shorten the scan time, you can select the object type to be scanned, i.e. determine which file formats the application should scan for malicious code.

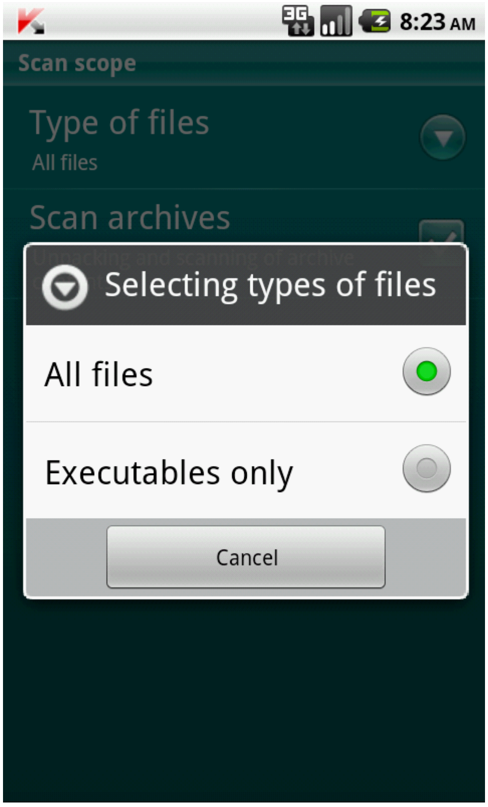
➧ *To select objects to be scanned:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Select **Scan settings** → **Scan scope**.

   The **Scan scope** screen opens.
4. Select a value for the **Type of files** setting (see fig. below):

   - **All files** - scan all types of files.
   - **Executables only** – scan only executable application files of the following formats: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.



Scan scope

Type of files: All files

Scan archives: Unpacking and scanning of archive

Selecting types of files

● All files

○ Executables only

Figure 13. Selecting the file types to scan

CONFIGURING ARCHIVE SCANS

Viruses often hide in archives. The program scans the following archive formats: ZIP, JAR, JAD, SIS SISX, CAB and APK. Archives are unpacked during scanning which may significantly reduce the speed of the Scan on Demand.

You can enable / disable the scan of archive for malicious code during the Scan on Demand.

➧ *To enable scan of archives:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** folder.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Select **Scan settings** → **Scan scope**.

   The **Scan scope** screen opens.
4. Check the **Scan archives** box.

SELECTING THE ACTION TO BE PERFORMED ON DETECTED OBJECTS

By default, if a threat is threat detected, Kaspersky Endpoint Security 8 for Smartphone attempts to disinfect it; if disinfection fails, the application deletes it. You can configure the actions that the application performs on detection of a threat.

➧ *To change how the application acts on the detected malicious object:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

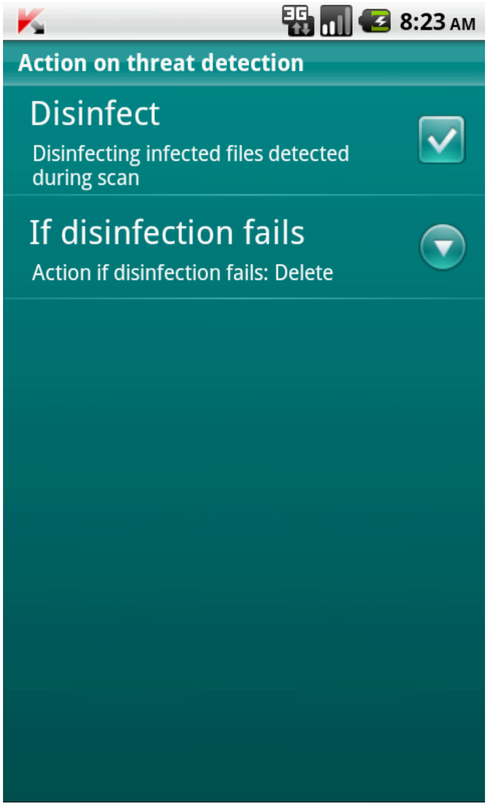
   The **Anti-Virus: Additional** screen opens.
3. Select **Scan settings** → **Action when threat is detected**.

   The **Action when threat is detected** screen opens.

4. Set the first action to be performed on a detected threat. Check the **Disinfect** box if you want the application first to attempt to disinfect the threat. Uncheck the **Disinfect** box if you do not want the application to attempt to disinfect the threat.

5. Set the second action to be performed by the application, if the threat cannot be disinfected. To do this, select a value for the **If disinfection fails** setting (see Figure below).

   - **Ask user**: prompt the user for actions when a malicious object is detected.
   - **Delete**: delete malware objects without notifying the user.
   - **Skip** – skip malicious objects without deleting them from the device.



Action on threat detection

Disinfect ☑
Disinfecting infected files detected during scan

If disinfection fails
Action if disinfection fails: Delete

Figure 14. Selecting the action to be performed on malicious objects if disinfection is not possible

QUARANTINING MALWARE OBJECTS

This section provides information on the *quarantine*, a special folder where potential malicious objects are placed. This section also describes how to view, restore or delete malicious objects found in the folder.

IN THIS SECTION

ABOUT QUARANTINE

While a device is being scanned or if Protection is enabled, the application places any malicious objects detected in *quarantine*, in a special isolated folder. Quarantined objects are stored in a packed format which prevents their activation, and thus they pose no threat to the device.

You can view files placed in quarantine, delete or restore them.

VIEWING QUARANTINED OBJECTS

You can view the list of malicious objects that the application has moved to Quarantine. For every object, its full name and date of detection are specified on the list.

You can also view additional information about the malicious object that you have selected: path to the object in the device before the application moved it to quarantine and name of the threat.

➡ *To view the list of objects in quarantine:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Tap **Quarantine**.

   The **Quarantine** screen, which contains the list of quarantined files, opens.

RESTORING OBJECTS FROM QUARANTINE

If you are sure that the object detected does not represent a threat to the device, you can restore it from quarantine. The restored object is placed in the original folder.

➧ *To restore an object from quarantine:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Tap **Quarantine**.

   This will open the **Quarantine** window.
4. Select a file to restore and tap **Menu** → **Restore**.

The selected file will be restored from Quarantine into its original folder.

DELETING OBJECTS FROM QUARANTINE

You can delete a single object or all the objects in quarantine.

➧ *To delete an object from Quarantine:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Tap **Quarantine**.

   This will open the **Quarantine** window.
4. Select an object to be deleted and then press **Menu** → **Delete**.

The selected object will be deleted from Quarantine.

➧ *To delete all quarantined objects:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** folder.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Tap **Quarantine**.

   This will open the **Quarantine** window.
4. Press **Menu** → **Delete all**.

All quarantined objects will be deleted.

FILTERING OF INCOMING CALLS AND SMS

This section contains information about Anti-Spam, which prevents unwanted calls and SMS according to the Black and White Lists you create. The section also describes how to select the mode, which Anti-Spam uses to check incoming calls and SMS messages, how to configure additional filtering settings for incoming SMS messages and calls and also how to create Black and White Lists.

IN THIS SECTION

ABOUT ANTI-SPAM

Anti-Spam blocks unwanted calls and SMS based on the user-defined White and Black Lists.

The lists consist of entries. An entry in either list contains the following information:

- The phone number, information from which Anti-Spam blocks for the Black List and delivers for the White List.
- The type of events that Anti-Spam blocks for the Black List and allows for the White List. The following types of communications are available: calls and SMS, calls only, and SMS only.
- Key phrase used by Anti-Spam to recognize wanted and unwanted SMS. For the Black List, Anti-Spam blocks SMS messages, which contain this phrase, while delivering the ones, which do not contain it. For the White List, Anti-Spam allows SMS, where this phrase is found and blocks SMS, which do not contain it.

Anti-Spam filters incoming SMS messages and calls in accordance with the selected mode (see "About Anti-Spam modes" on page 39). According to the mode, Anti-Spam checks every incoming SMS or call and then determines whether this SMS or call is wanted or unwanted (spam). As soon as Anti-Spam assigns the wanted or unwanted status to an SMS or call, the scan is finished.

Information about blocked SMS messages and calls is recorded in the Anti-Spam Log (see "Viewing Log records" on page 49).

ABOUT ANTI-SPAM MODES

The selected mode defines the rules according to which Anti-Spam filters incoming calls and SMS messages.

The following Anti-Spam modes are available:

- **Off** – all incoming calls and SMS are allowed.
- **Black List** – all calls and SMS are allowed in except for those originating from numbers on the Black List.
- **White List** – only calls and SMS originating from numbers on the White List are allowed in.
- **Both lists** – incoming calls and SMS from White List numbers are allowed while those from Black List numbers are blocked. Following a conversation or arrival of an SMS message from a number on neither list, Anti-Spam will prompt the user to add the number to one of the lists.

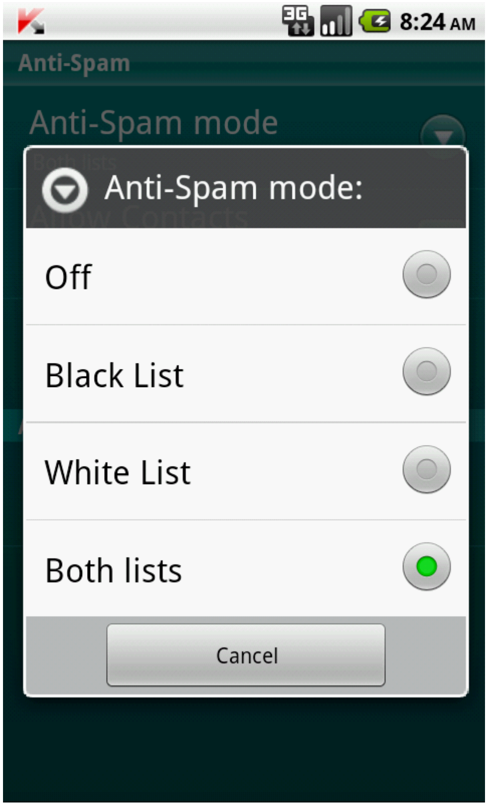
You can change the current Anti-Spam mode (see section "Changing the Anti-Spam mode" on page 39). Current Anti-Spam mode is indicated on the **Anti-Spam** tab next to the **Mode** menu item.

CHANGING THE ANTI-SPAM MODE

To change the Anti-Spam mode:

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Mode: <current mode of component>**.

   The **Anti-Spam** screen will open.
3. Select the appropriate value for the **Anti-Spam** settings (see figure below).



Anti-Spam mode:

○ Off

○ Black List

○ White List

● Both lists

Figure 15. Changing the Anti-Spam mode

CREATING A BLACK LIST

The Black List contains entries of banned numbers, i.e., the numbers, from which Anti-Spam blocks calls and SMS. Each entry contain the following information:

- Phone number from which Anti-Spam blocks calls and (or) SMS.
- Type of events invoked from the number that Anti-Spam blocks. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase that Anti-Spam uses to classify an SMS message as unsolicited (spam). Anti-Spam only blocks SMS messages containing this key phrase while delivering all the rest.

Anti-Spam will block those calls and SMS that satisfy all the criteria of a Black List entry. Calls and SMS that fail to satisfy even one of the criteria in a Black List entry will be allowed in by Anti-Spam.

It is impossible to add the same phone number with the same filter criteria to the Black and White lists.

Information about blocked SMS messages and calls is recorded in the Anti-Spam Log (see "Viewing Log records" on page 49).

IN THIS SECTION

ADDING ENTRIES TO THE BLACK LIST

Bear in mind that the same number with identical filtering criteria cannot be included in the Black and White lists of Anti-Spam numbers at the same time. If a number with such filtering criteria is already saved on either of the lists, Kaspersky Endpoint Security 8 for Smartphone notifies you of this event, and a relevant message appears on the screen.

➧ *To add an entry to the Anti-Spam Black List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Black List**.

   This opens the **Black List** screen.
3. Tap **Add** (see Figure below).

4. Set values with the following settings:

   - **Block incoming** – type of events invoked from a phone number, which Anti-Spam blocks for the numbers from Black List:

     - **SMS** – block incoming SMS messages only.
     - **Calls** – block incoming calls only.
     - **Calls and SMS**: block incoming calls and SMS messages.

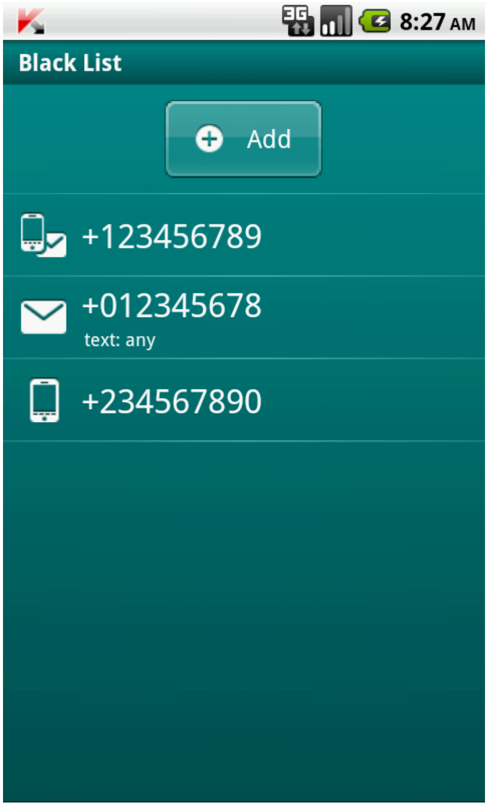
   - **Blocked phone number** – telephone number, for which Anti-Spam blocks incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any number of symbols, and "?" any symbol). For example, *1234? is in the Black List. Anti-Spam blocks calls or SMS from a number, in which any symbol follows the digits 1234.

   - **Blocked text** – a key file indicating that an incoming SMS is unsolicited (spam). Anti-Spam only blocks SMS messages containing the key phrase and delivers all others.

     The setting is available for the **SMS** event type.

     If you want all SMS messages to be blocked from a number in the Black List, leave the **Blocked text** field for this entry blank.

5. Tap **Save**.



8:27 AM

Black List

Add

+123456789

+012345678
text: any

+234567890

Figure 16. Adding entries to the Black List

EDITING ENTRIES IN THE BLACK LIST

You can change the values of all settings for entries from the Black List.

➡ *To edit an entry in the Anti-Spam Black List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Black List**.

   This opens the **Black List** screen.

3. Select the entry from the list that you want to change, and in the context menu for the entry select **Edit**.
4. Change the necessary settings:

   - **Blocked phone number** – telephone number, for which Anti-Spam blocks incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any number of symbols, and "?" any symbol). For example, *1234? is in the Black List. Anti-Spam blocks calls or SMS from a number, in which any symbol follows the digits 1234.
   - **Blocked text** – a key file indicating that an incoming SMS is unsolicited (spam). Anti-Spam only blocks SMS messages containing the key phrase and delivers all others.

     The setting is available for the **SMS** event type.

   > If you want all SMS messages to be blocked from a number in the Black List, leave the **Blocked text** field for this entry blank.

5. Tap **Save**.

DELETING ENTRIES FROM THE BLACK LIST

You can delete a number from the Black list. Furthermore, you can clear the Anti-Spam Black List by removing all the entries from it.

➡ *To delete an entry from the Anti-Spam Black List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Black List**.

   This opens the **Black List** screen.

3. In the list, select the entry that you want to delete, and in the context menu for the entry select **Delete**.

➡ *To clear the Anti-Spam Black List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Black List**.

   This opens the **Black List** screen.

3. In the context menu, select **Delete all**.

   The confirmation window opens.

4. Confirm the uninstalling by pressing the **Yes** button.

The list is emptied.

CREATING A WHITE LIST

The White List contains entries of allowed numbers, i.e., numbers from which Anti-Spam delivers calls and SMS to the user. Each entry contain the following information:

- Phone number, from which Anti-Spam delivers calls and (or) SMS.
- Type of events invoked from the number that Anti-Spam allows. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase used by Anti-Spam to classify an SMS message as solicited (not spam). Anti-Spam only delivers SMS messages containing the key phrase and blocks all others.

Anti-Spam allows only calls and SMS that satisfy all the criteria of an entry in the White List. Calls and SMS that fail to satisfy even one of the criteria in a White List entry will be blocked by Anti-Spam.

IN THIS SECTION

ADDING ENTRIES TO THE WHITE LIST

Bear in mind that the same number with identical filtering criteria cannot be included in the Black and White lists of Anti-Spam numbers at the same time. If a number with such filtering criteria is already saved on either of the lists, Kaspersky Endpoint Security 8 for Smartphone notifies you of this event, and a relevant message appears on the screen.

➡ *To add an entry to the the Anti-Spam White List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **White List**.

   This opens the **White List** screen.
3. Tap **Add** (see Figure below).

4. Apply the following settings for the new entry:

   - **Allow incoming** – type of events invoked from a phone number, which Anti-Spam allows for White List numbers:

     - **SMS** – allow incoming SMS messages only.
     - **Calls** – allow incoming calls only.
     - **Calls and SMS**: allow incoming calls and SMS.

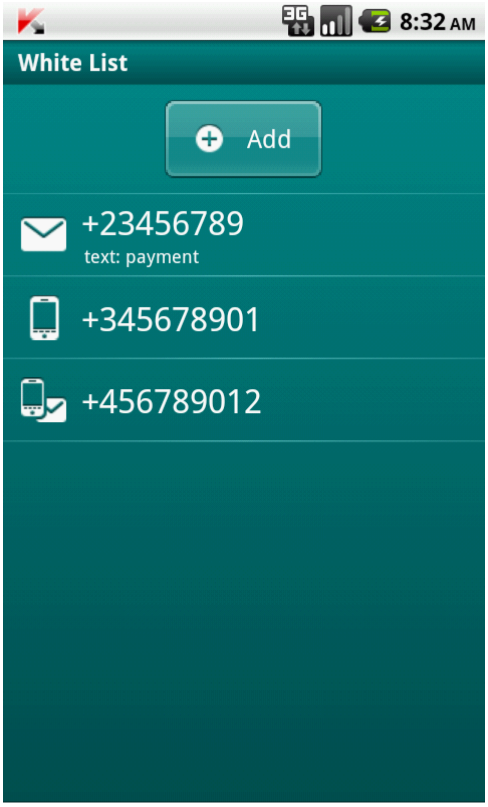
   - **Allowed phone number** – phone number, from which Anti-Spam delivers incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any number of symbols, and "?" any symbol). For example, *1234? is in the White List. Anti-Spam allows in calls or SMS from a number, in which any symbol follows the digits 1234.

   - **Allowed text** – key phrase indicating that the received SMS message is solicited. For numbers on the White List, Anti-Spam only delivers SMS messages containing the key phrase and blocks all others.

     The setting is available for the **SMS** event type.

     If you want all incoming SMS from a specific number on the White List to be delivered, leave the **Allowed text** field of this entry blank.

5. Tap **Save**.



+23456789
text: payment

+345678901

+456789012

Figure 17. Adding entries to the White List

EDITING ENTRIES IN THE WHITE LIST

For an entry from the White List of allowed numbers, you can change the values of all settings.

➧ *To edit an entry in the Anti-Spam White List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **White List**.

   This opens the **White List** screen.

3. Select the element from the list that you want to change, and in the context menu for the entry select **Edit**.
4. Change the necessary settings:
   - **Allowed phone number** – phone number, from which Anti-Spam delivers incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any number of symbols, and "?" any symbol). For example, *1234? is in the White List. Anti-Spam allows in calls or SMS from a number, in which any symbol follows the digits 1234.
   - **Allowed text** – key phrase indicating that the received SMS message is solicited. For numbers on the White List, Anti-Spam only delivers SMS messages containing the key phrase and blocks all others.

     The setting is available for the **SMS** event type.

     If you want all incoming SMS from a specific number on the White List to be delivered, leave the **Allowed text** field of this entry blank.

5. Tap **Save**.

DELETING ENTRIES FROM THE WHITE LIST

You can delete one entry from the White List as well as completely clear it.

➧ *To delete an entry from the Anti-Spam White List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **White List**.

   This opens the **White List** screen.

3. In the list, select the entry that you want to delete, and in the context menu for the entry select **Delete**.

➧ *To clear the Anti-Spam White List:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **White List**.

   This opens the **White List** screen.

3. In the context menu, select **Delete all**.

   The confirmation window opens.

4. Confirm the uninstalling by pressing the **Yes** button.

The White List becomes empty.

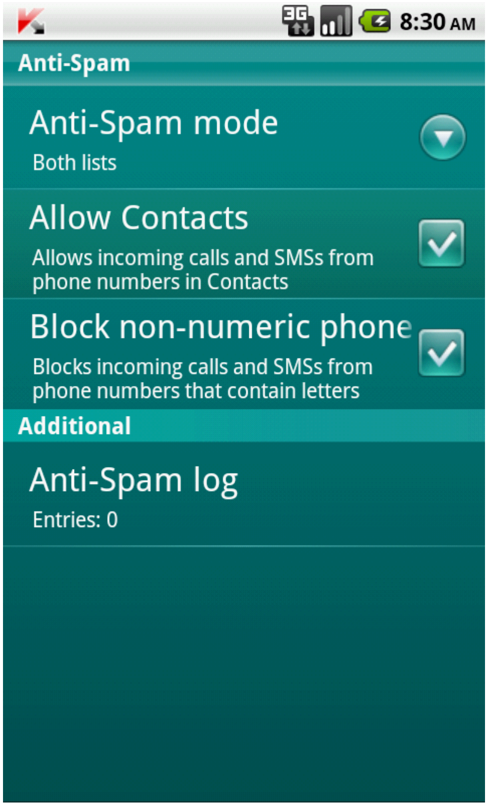
RESPONDING TO SMS MESSAGES AND CALLS FROM CONTACTS NOT IN THE PHONE BOOK

For the **Both lists** or **White List** mode, you can additionally set up Anti-Spam response to SMS messages and calls from senders whose numbers are not present in Contacts. Anti-Spam also allows expansion of the White List by adding numbers from the Contacts to it.

➧ *To select Anti-Spam response to a number not included in the phonebook:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Mode: <current mode of component>**.

   The **Anti-Spam** screen will open.
3. Select the required value for setting **Allow Contacts** (see Figure below).
   - to make Anti-Spam consider numbers from Contacts as an additional White List and block SMS messages and calls from senders not in Contacts, check the **Allow Contacts** box;
   - to make Anti-Spam filter SMS messages and calls based on the selected mode only, uncheck the **Allow Contacts** box.



8:30 AM

Anti-Spam

Anti-Spam mode
Both lists

Allow Contacts ☑
Allows incoming calls and SMSs from phone numbers in Contacts

Block non-numeric phone ☑
Blocks incoming calls and SMSs from phone numbers that contain letters

Additional

Anti-Spam log
Entries: 0

Figure 18. Anti-Spam response to numbers not found in Contacts

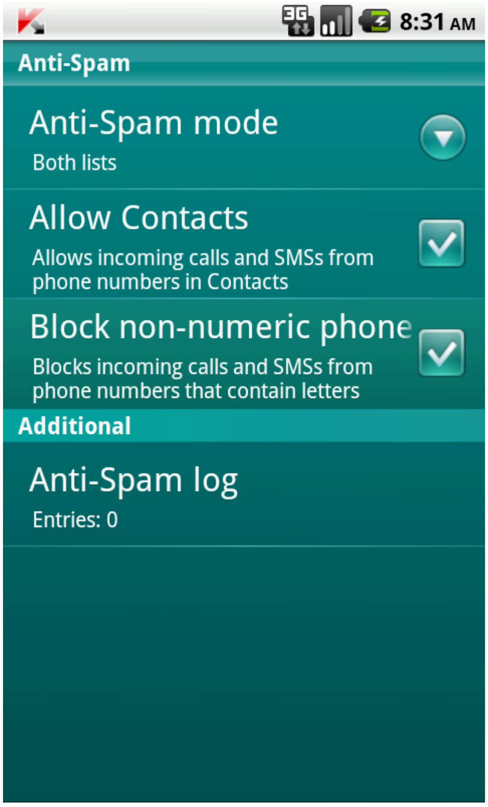
RESPONDING TO SMS MESSAGES FROM NON-NUMERIC NUMBERS

For the **Both lists** or **Black List** Anti-Spam modes, you can expand the Black List by adding all non-numeric numbers (containing letters) to it. In this case, Anti-Spam treats SMS messages from non-numeric numbers in the same way as from numbers on the Black List.

➧ *To configure Anti-Spam response upon arrival of SMS messages from non-numeric numbers:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Mode: <current mode of component>**.

   The **Anti-Spam** screen will open.
3. Select a value for the **Block non-numeric numbers** setting (see Figure below).
   - in order for Anti-Spam to automatically block SMS from non-numeric numbers, check the **Block non-numeric numbers** box;
   - to make Anti-Spam check SMS from non-numeric numbers based on the selected mode only, uncheck the **Block non-numeric numbers** box.



8:31 AM

Anti-Spam

Anti-Spam mode
Both lists

Allow Contacts ☑
Allows incoming calls and SMSs from phone numbers in Contacts

Block non-numeric phone ☑
Blocks incoming calls and SMSs from phone numbers that contain letters

Additional

Anti-Spam log
Entries: 0

Figure 19. Selecting Anti-Spam response upon arrival of SMS from a non-numeric number

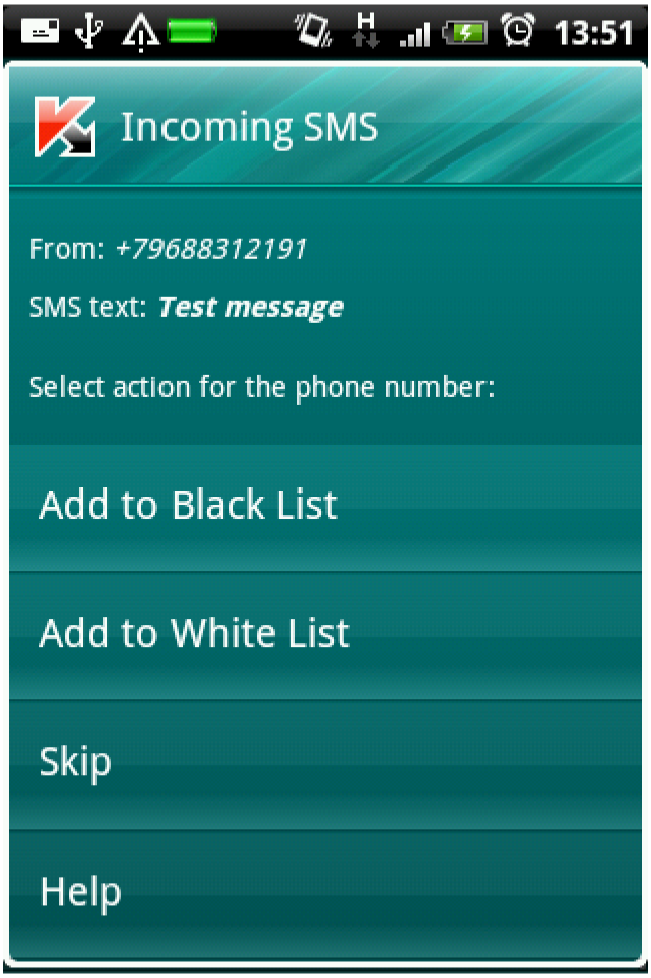
SELECTING A RESPONSE TO INCOMING SMS

In the **Both lists** mode, Anti-Spam scans incoming SMS messages against the Black and White lists.

Following arrival of an SMS message from a number on neither list, Anti-Spam will prompt the user to add the number to one of the lists (see figure below).

You can select one of the following actions for an SMS:

- To block an SMS and add a sender's phone number to the Black List tap **Add to Black List**.
- To receive an SMS and add a sender's phone number to the White List tap **Add to White List**.
- To deliver the SMS message without adding the sender's telephone number to either list, press **Skip**.



From: +79688312191

SMS text: ***Test message***

Select action for the phone number:

Figure 20. Anti-Spam notification about received SMS

Information about blocked SMS messages is recorded in the Anti-Spam Log (see "Viewing Log records" on page 49).

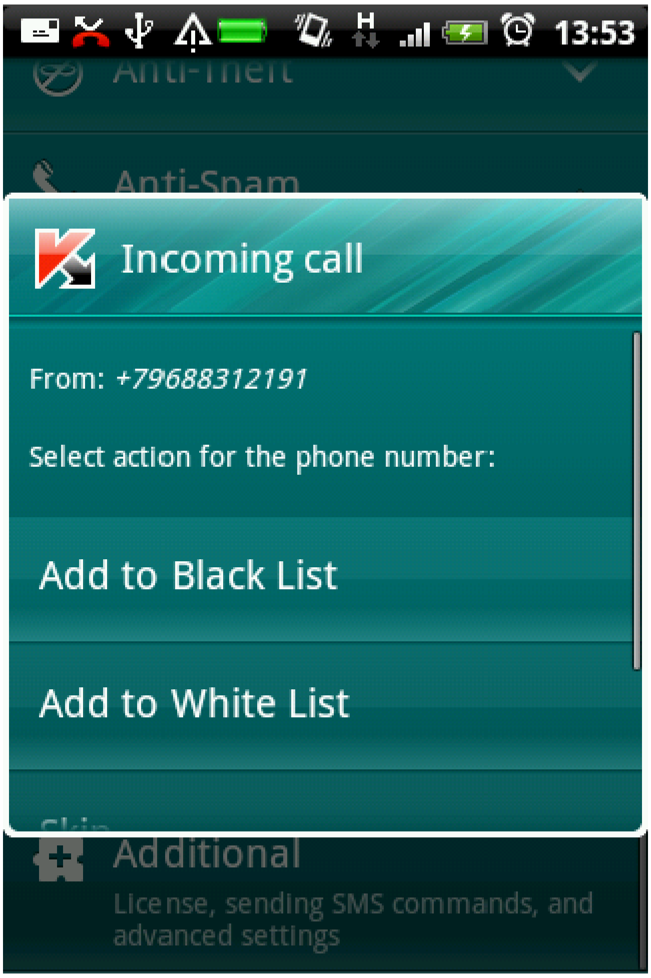
SELECTING A RESPONSE TO INCOMING CALLS

In the **Both lists** mode, Anti-Spam checks incoming calls against the Black and White lists. Following a call from a number on neither list, Anti-Spam will prompt the user to add the number to one of the lists (see figure below).

You can select one of the following actions for the caller's number:

- To add the caller's telephone number to the Black List, tap **Add to Black List**.
- To add the caller's telephone number to the White List, tap **Add to White List**.
- If you don't want to add the caller's number to either list, press **Skip**.

Information about blocked calls is recorded in the Anti-Spam Log (see "Viewing Log records" on page 49).



13:53

Anti-Theft

Anti-Spam

Incoming call

From: *+79688312191*

Select action for the phone number:

Add to Black List

Add to White List

Skip

Additional

License, sending SMS commands, and advanced settings

Figure 21. Anti-Spam notification about received call

VIEWING LOG RECORDS

You can view information about blocked calls and SMS messages in the Anti-Spam Log. Entries in the log are sorted in reverse chronological order.

The following information is provided on each entry:

- Phone number that invoked an event blocked by Anti-Spam.
- The date it was blocked.
- The time it was blocked.

➧ *To view information about blocked calls and SMS messages:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Spam** section.
2. Select **Mode: <current mode of component>**.

   The **Anti-Spam** screen will open.
3. In the **Additional** section select **Events log** item.

The **Anti-Spam log** screen will open.

➧ *To view detailed information about a blocked event,*

select the required entry in the Log.

DATA PROTECTION IN THE EVENT OF DEVICE LOSS OR THEFT

This section gives information about Anti-Theft which, in the case of theft or loss, blocks unauthorized access to data saved on your mobile device and makes it easy to find the device.

This section also specifies how to enable/disable the Anti-Theft function, set its parameters and start Anti-Theft from another mobile device remotely.

IN THIS SECTION

ABOUT ANTI-THEFT

Anti-Theft protects information stored on your mobile device from unauthorized access.

Anti-Theft includes the following functions:

- **Block** – allows blocking the device remotely and gives the text to be displayed on the screen of the blocked device.

- **Date Wipe** – allows the user's personal data (entries in Contacts and on the SIM card, SMS messages, call history, calendar, Internet connection settings, user accounts, except for the Google™ account) to be deleted remotely, and also folders from the list for deletion.

> Kaspersky Endpoint Security 8 for Smartphone only deletes contacts on the SIM card on devices running version 2.0 or above of the Android operating system.

- **SIM Watch** allows obtaining the current phone number or locking the device, if the SIM card is replaced or the device is activated without a SIM card. Information about a new phone number is sent as a message to the phone number and / or email that you specified.

- The **GPS Find** functionality enables you to locate a device. The geographical coordinates of the device are sent as a message to the phone number from which a special SMS command was sent, and to an email address.

Following installation of Kaspersky Endpoint Security 8 for Smartphone, all Anti-Theft functions are disabled.

Kaspersky Endpoint Security 8 for Smartphone can remotely start Anti-Theft with sending SMS commands from another mobile device (see "Remote start of the Anti-Theft functions" on page 59).

To start Anti-Theft remotely, you must know the application secret code that was set when Kaspersky Endpoint Security 8 for Smartphone was first started.

The current status of each function is displayed on the Home screen in the **Anti-Theft** section next to the name of the function.

BLOCKING THE DEVICE

After a special SMS command is received, the Block function allows you to remotely block access to the device and data stored on it. The device can only be unblocked by entering the secret code.

This function does not block the device but simply enables the remote blocking option.

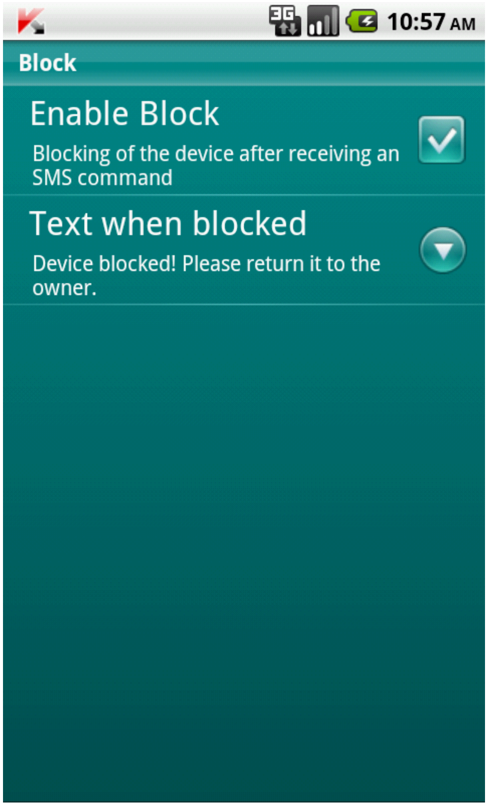
For the Block function to work on an Android OS device, Kaspersky Endpoint Security 8 for Smartphone needs to be installed with the Default Home screen.

If the application is not installed with the Default Home screen, protection of device during activation of the Block function cannot be guaranteed. To install Kaspersky Endpoint Security 8 for Smartphone with the Default Home screen, you should reset the configuration of the current default screen.

➨ *To enable the Block function:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Theft** folder.
2. Tap **Block**: **<current status of function>**.

   This opens the **Block** screen.
3. Check the **Enable Block** box.
4. Enter the message displayed on the device screen in blocked mode in the **Text when blocked** field (see figure below). By default, the standard text in which you can add the owner's phone number is used for the message.



Enable Block ☑
Blocking of the device after receiving an SMS command

Text when blocked
Device blocked! Please return it to the owner.

Figure 22. Block feature settings

If the Block function is enabled on another device, you can block it using any of the following methods:

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8 for Smartphone, on another mobile device to create and send an SMS command to your device. To create a special SMS command, use the **Send command** function. As a result, your device will receive a covert SMS, and the device will be blocked.
- On another mobile device, create and send an SMS with the special text and the secret code previously set for the receiving device.

Outgoing SMS messages are billed according to the rates set by the mobile service provider of the other mobile device.

To block the device remotely, it is advised that you use the secure method with the Sending a command function. The application secret code is then sent in encrypted form.

➧ *To send an SMS command to another device using the Send command function:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.

   This will open the **Additional** window.
2. Select **Send SMS command**.
3. Select the value **Block** for the **SMS command** setting.
4. In the **Phone number that received SMS command** field, enter the telephone number of the device that received the SMS command.
5. In the **Secret code that received SMS command** field, enter the secret code of the application specified on the device that received the SMS command.
6. Press **Send**.

➧ *To create an SMS using the phone standard SMS creation functionality:*

send an SMS message from the other device containing the text `block:<code>`, where `<code>` is the secret code set on the device to be blocked. The message is not case sensitive, and spaces before or after the colon are ignored.

DELETING PERSONAL DATA

After a special SMS command is received, the Data Wipe function allows deleting the following information stored in the device:

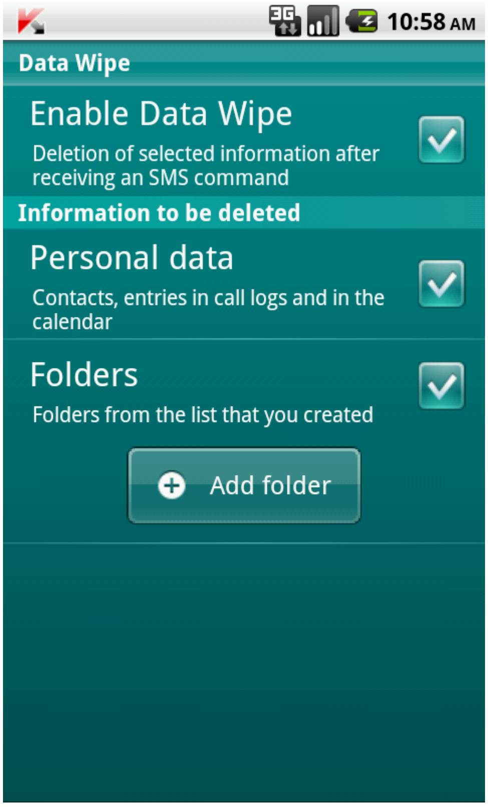
- the user's personal data (entries in Contacts and on the SIM card, SMS messages, call history, calendar, Internet connection settings, user accounts, except for the Google account);
- files from the list of folders for deletion saved on the storage card (see the "Creating a list of folders to delete" section on page 55).

This function does not delete the data saved on the device, but includes the option to delete them.

To enable the Data Wipe function:

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Theft** section.
2. Tap **Data Wipe**: **<current status of function>**.

   This opens the **Data Wipe** screen.
3. Check the **Enable Data Wipe** box.
4. Select information that you want to delete. To do so, in the **Information to be deleted** section, check the boxes next to the required settings (see fig. below):
   - to delete personal data, check the **Personal data** box;
   - to delete files from the list of folders for deletion, check the **Folders** box and then create a list of folders for deletion (see "Creating a list of folders to delete" on page 55).



10:58 AM

Data Wipe

Enable Data Wipe ☑

Deletion of selected information after receiving an SMS command

Information to be deleted

Personal data ☑

Contacts, entries in call logs and in the calendar

Folders ☑

Folders from the list that you created

Figure 23. Data Wipe settings

You can delete personal data from the device with the function enabled by using the following methods:

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8 for Smartphone, on another mobile device to create and send an SMS command to your device. As a result, your device receives a covert SMS message and the information is deleted. To create a special SMS command, use the Send command function.
- On another mobile device, create and send an SMS with the special text and the secret code previously set for the receiving device. As a result, your device receives a covert SMS message and the information is deleted.

Outgoing SMS messages are billed according to the rates set by the mobile service provider of the other mobile device.

To delete information from the device remotely, you are advised to use the secure method with the Sending a command function. The application secret code is then sent in encrypted form.

➧ *To send an SMS command to another device using the Send command function:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

   This will open the **Additional** window.

2. Select **Send command**.
3. For the **SMS command** setting, select **Data Wipe**.
4. In the **Phone number that received SMS command** field, enter the telephone number of the device that received the SMS command.
5. In the **Secret code that received SMS command** field, enter the secret code of the application specified on the device that received the SMS command.
6. Press **Send**.

➧ *To create an SMS with the phone standard SMS creation functions:*

from another telephone, send an SMScontaining the text **wipe:<code>**, where **<code>** is the application secret code set on the target device. The message is not case sensitive, and spaces before or after the colon are ignored.

CREATING A LIST OF FOLDERS TO DELETE

The Data Wipe function allows creating a list of folders to be deleted after a special SMS command is received. You are able to select folders saved on a storage card.

If you want Anti-Theft to delete the folders from the list after receiving a special SMS command, make sure that the **Folders** box in the Data Wipe settings is checked.

➧ *To add a folder to the list of folders to be deleted:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Theft** folder.
2. Tap **Data Wipe**.

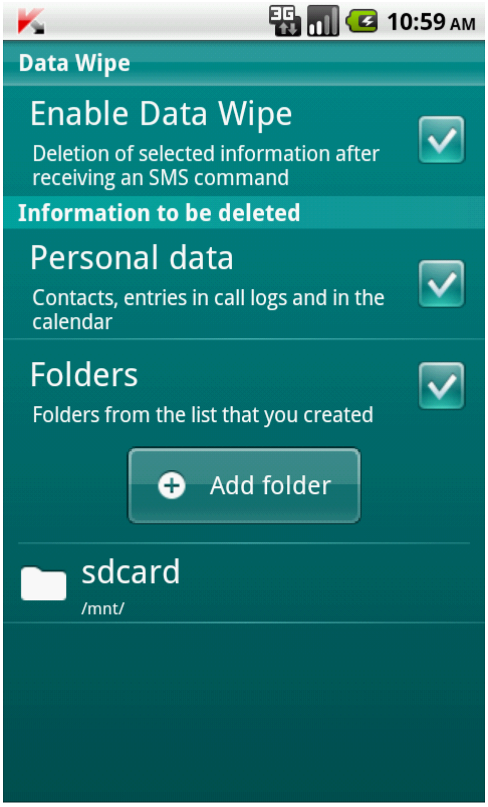
   This opens the **Data Wipe** screen.

3. Tap **Add folder** (see fig. below).

   The **Folder selection** screen opens.

4. Select the required folder by tapping the icon to the right of the name of the folder.

   The folder is added to the list of folders for deletion, located below the **Folders** settings.



10:59 AM

Data Wipe

Enable Data Wipe ☑
Deletion of selected information after receiving an SMS command

Information to be deleted

Personal data ☑
Contacts, entries in call logs and in the calendar

Folders ☑
Folders from the list that you created

Add folder

sdcard
/mnt/

Figure 24. Adding a folder

➨ *To remove a folder from the list:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Theft** folder.
2. Tap **Data Wipe**.

   This opens the **Data Wipe** screen.
3. Go to the list of objects for deletion.
4. Select the folder from the list, and tap **Delete** in the context menu.

   The folder is deleted from the list of folders for deletion.

MONITORING THE REPLACEMENT OF A SIM CARD ON THE DEVICE

If the SIM card is replaced, SIM Watch allows you to send a message with the new number to your phone number and / or email, or lock the device.

➡ *To enable the SIM Watch function and monitor the replacement of the SIM card:*

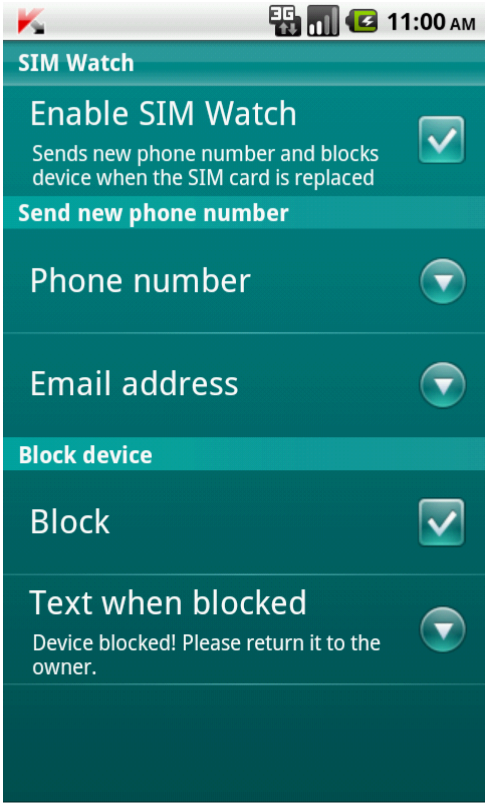
1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Theft** section.
2. Tap **SIM control**: **<current status of component>**.

   This opens the **SIM Watch** screen.
3. Check the **Enable SIM Watch** box.
4. To check the replacement of the SIM card on the device, make the following settings (see Figure below).
   - To automatically receive an SMS with the new number of your telephone, in the **Phone number** field in the **Send new number** section, enter the telephone number to which the SMS is to be sent.

     The phone number may start with a digit or with a "+", and must contain digits only.
   - To receive an email message with the new telephone number, in the **Email address** field in the **Send new number** section, enter the email address.
   - To block the device if the SIM card is replaced, or if the device is turned on with the SIM card removed, check the **Block** box in the **Additional** block. You can unblock the device only by entering the application secret code.
   - To display an onscreen message in blocked mode, in the **Text when blocked** field in the **Additional** section, enter the text of the message.

     By default, the standard text in which you can add the owner's number is used for the message.

     The setting is available if the **Block** box is checked.



11:00 AM

SIM Watch

Enable SIM Watch ☑

Sends new phone number and blocks device when the SIM card is replaced

Send new phone number

Phone number

Email address

Block device

Block ☑

Text when blocked

Device blocked! Please return it to the owner.

Figure 25. SIM Watch settings

DETERMINING THE DEVICE GEOGRAPHICAL COORDINATES

After a special SMS command is received, GPS Find allows detecting the device geographical coordinates and sending them by SMS and email to the requesting device and an email address.

Outgoing SMS messages are billed according to your mobile service provider's current rate.

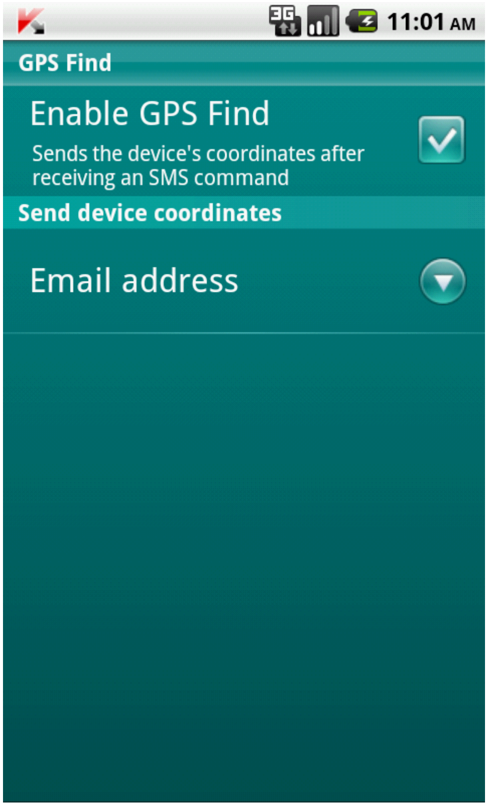
If the device has a built-in GPS receiver, it will be automatically enabled after the device receives a special SMS command. If GPS Find cannot receive the device's coordinates, it determines the approximate coordinates of the device using base stations.

➧ *To enable the GPS Find function:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Theft** folder.
2. Tap **GPS Find**: **<current status of component>**.

   This opens the **GPS Find** screen.
3. Check the **Enable GPS Find** box.

   On receipt of a special SMS command, Kaspersky Endpoint Security 8 for Smartphone automatically sends the coordinates of the device in an SMS reply to the number from which the SMS command was sent.
4. To receive the coordinates of the device by email as well, in the **Email address** field in the **Send device coordinates** section, enter the email address (see fig. below).



GPS Find

Enable GPS Find ☑
Sends the device's coordinates after receiving an SMS command

Send device coordinates

Email address

Figure 26. GPS Find settings

You can request the coordinates of a device on which GPS Find is enabled, using the following methods:

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8 for Smartphone, on another mobile device to create and send an SMS command to your device. As a result, your device will receive a covert SMS, and the application will send the device coordinates. To create a special SMS command, use the Send command function.
- On another mobile device, create and send an SMS with the special text and the secret code previously set for the receiving device. As a result, your device will receive the SMS, and the application will send the coordinates of the device.

Outgoing SMS messages are billed according to the rates set by the mobile service provider of the other mobile device.

To receive the device coordinates, you are advised to use the secure method with the Send command function. The application secret code is then sent in encrypted mode.

➧ *To send a command to another device using the Send command function:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

   This will open the **Additional** window.

2. Tap **Send command**.
3. Select the **GPS Find device** value for the **SMS command** setting.
4. In the **Phone number that received SMS command** field, enter the telephone number of the device that received the SMS command.
5. In the **Secret code that received SMS command** field, enter the secret code of the application specified on the device that received the SMS command.
6. Press **Send**.

➧ *To create an SMS using the standard SMS creation functionality:*

send an SMS to another device; it should contain the text **find:<code>**, where **<code>** is the application secret code set on the target device. The message is not case sensitive, and spaces before or after the colon are ignored.

An SMS with the device coordinates will be sent to the phone number from which the SMS command was sent and to the email address if you have specified one in the GPS Find options.

REMOTE START OF THE ANTI-THEFT FUNCTIONALITY

The application allows sending a special SMS command to run Anti-Theft functions remotely on another device with Kaspersky Endpoint Security 8 for Smartphone installed on it. An SMS command is sent as an encrypted SMS and contains the application secret code set on the other device. Reception of the SMS command will not be noticed.

SMS is billed according to your mobile service provider's current rate.

➡ *To send an SMS command to another device:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.
2. Select the function for remote launch on another mobile device. Select one of the proposed values for the **SMS command** setting (see Figure below).
   - **Block**;
   - **Data Wipe**;
   - **GPS Find**;
   - **Hide information**.
3. In the **Phone number that received SMS command** field, enter the telephone number of the device that received the SMS command.
4. In the **Secret code that received SMS command** field, enter the secret code of the application specified on the device that received the SMS command.
5. Press **Send**.

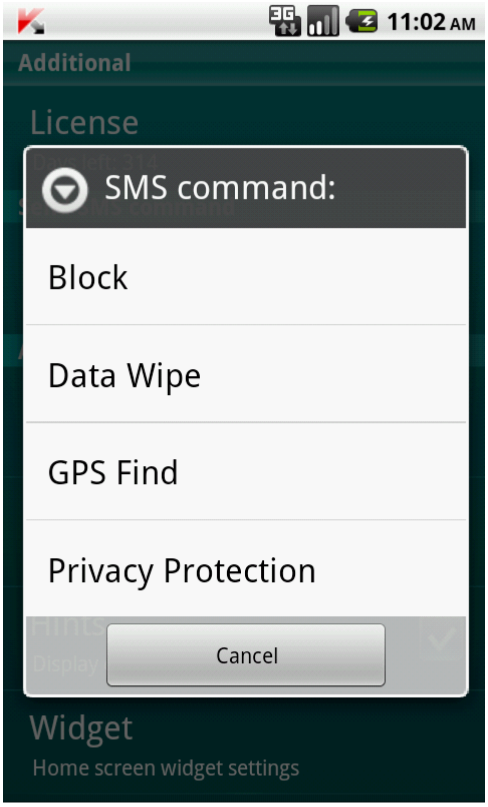


Figure 27. Remote startup of Anti-Theft and Privacy Protection features

PRIVACY PROTECTION

The section presents information about Privacy Protection, which can hide the user's confidential information.

IN THIS SECTION

PRIVACY PROTECTION

Privacy Protection hides private data based on your Contact list, which lists private numbers. For confidential numbers, Privacy Protection hides Contacts entries, incoming, drafts, and sent SMS as well as call history entries. Privacy Protection suppresses the new SMS signal and hides the message itself in the inbox. Privacy Protection blocks incoming calls from private numbers and does not display incoming call information on the screen. As a result, the caller receives a busy signal. To view incoming calls and SMS for the period of time when Privacy Protection was enabled, disable Privacy Protection. On the repeat enabling of Privacy Protection, the information is not displayed.

You are able to activate Privacy Protection from Kaspersky Endpoint Security 8 for Smartphone or remotely from another mobile device. However, Privacy Protection can only be disabled from within the application.

PRIVACY PROTECTION MODES

You can manage the operation mode of Privacy Protection. The mode defines whether Privacy Protection is enabled or disabled.

By default, Privacy Protection is disabled.

The following modes of Privacy Protection are available:

- **Confidential information is displayed** – Privacy Protection is disabled. The Privacy Protection settings are accessible for modification.
- **Confidential information is hidden** – Privacy Protection is enabled. The Privacy Protection settings cannot be changed.

You can configure automatic activation of confidential data hiding (see 62) or remote activation of confidential data hiding (see section "Enabling Privacy Protection remotely" on page 64).

The current mode of displaying or hiding confidential information is displayed in the **Privacy Protection** section.

CHANGING THE PRIVACY PROTECTION MODE

➡ *To change the Privacy Protection mode:*

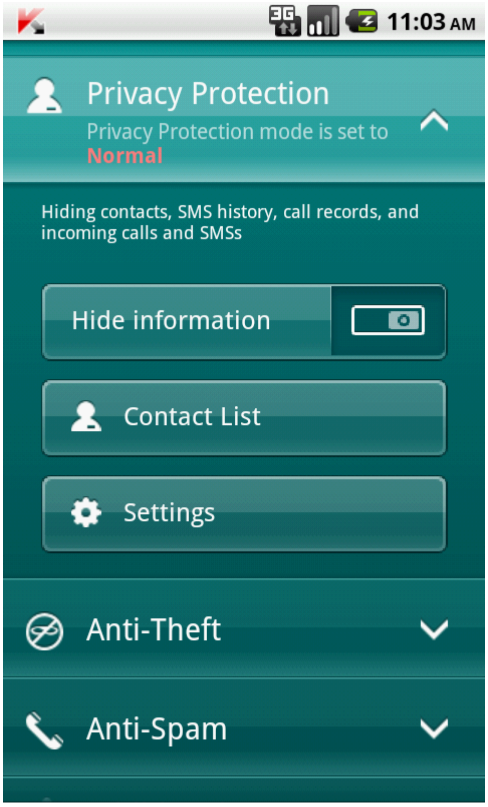
1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection**.
2. Tap **Hide information** (see fig. below).

   The name of the item changes in accordance with the Privacy Protection mode. If the **Confidential information is displayed** mode is set, the item is named **Hide information**. If the **Confidential information is hidden** mode is set, the item is named **Display information**.

Changing the mode of Privacy Protection can take some time.

The current Privacy Protection mode is displayed in the **Privacy Protection** section.

The icon switch to the right of the **Hide information** / **Display information** item changes in accordance with the selected mode.



11:03 AM
Privacy Protection
Privacy Protection mode is set to
Normal
Hiding contacts, SMS history, call records, and incoming calls and SMSs
Hide information
Contact List
Settings
Anti-Theft
Anti-Spam

Figure 28. Changing Privacy Protection mode

ENABLING PRIVACY PROTECTION AUTOMATICALLY

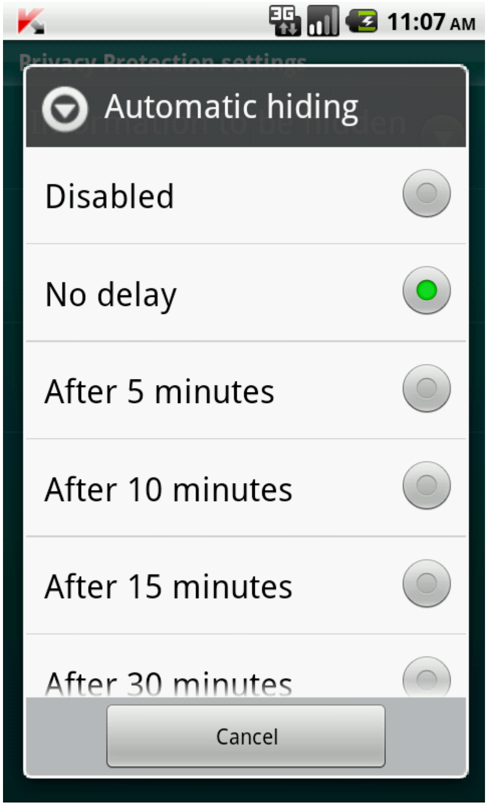
You can configure automatic enabling of hiding confidential information after a specified time interval. The function becomes activated after the device switches to power-saving mode.

Disable Privacy Protection prior to editing Privacy Protection settings.

➡ *To enable Privacy Protection automatically after a specified time interval elapses:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the the **Privacy Protection** section.
2. Tap **Settings**.

   The **Privacy Protection settings** screen opens.
3. Select a value for the **Hide automatically** setting in accordance with the following tasks (see fig. below):
   - To disable automatic enabling of Privacy Protection, select **Disabled**.
   - To enable Privacy Protection after a set period after the device switches to power-saving mode, select one of the following values:
     - **No delay**.
     - **After 1 minute**.
     - **After 5 minutes**.
     - **After 10 minutes**.
     - **After 15 minutes**.
     - **After 30 minutes**.



Automatic hiding

Disabled ○

No delay ●

After 5 minutes ○

After 10 minutes ○

After 15 minutes ○

After 30 minutes ○

Figure 29. Automatic start settings for Privacy Protection

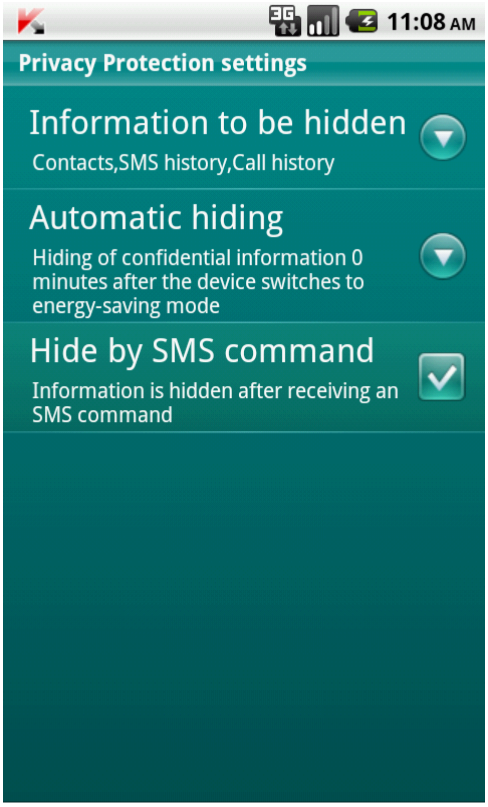
ENABLING PRIVACY PROTECTION REMOTELY

Kaspersky Endpoint Security 8 for Smartphone can start hiding confidential information remotely from another remote device. To accomplish this, first activate the **Hide on SMS command** option on your device.

➡ *To allow remote enabling of Privacy Protection:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection**.
2. Tap **Settings**.

   The **Privacy Protection settings** screen opens.
3. Check the **Hide on SMS command** box (see figure below).



Privacy Protection settings

Information to be hidden
Contacts,SMS history,Call history

Automatic hiding
Hiding of confidential information 0 minutes after the device switches to energy-saving mode

Hide by SMS command ☑
Information is hidden after receiving an SMS command

Figure 30. Remote activation settings for Privacy Protection

You can enable Privacy Protection remotely using any of the following methods:

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8 for Smartphone, on another mobile device to create and send an SMS command to your device. As a result, your device unnoticeably receives an SMS, and confidential information is hidden. To create a special SMS command, use the Send command function.
- On another mobile device, create and send an SMS message with a special text and the secret code of the application specified on your device. As a result, the device receives an SMS, and confidential information is hidden.

Outgoing SMS will be billed at the rates set by the mobile provider for the phone where the SMS command originates.

➧ *To start hiding confidential information remotely from another mobile device with the special SMS command:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.
2. This will open the **Additional** window.
3. Select **Send command**.
4. Select the value **Hide information** for the **SMS command** setting.
5. In the **Phone number that received SMS command** field, enter the telephone number of the device that received the SMS command.
6. In the **Secret code that received SMS command** field, enter the secret code of the application specified on the device that received the SMS command.
7. Press **Send**.

When an SMS command is received on the device, Kaspersky Endpoint Security 8 for Smartphone enables Privacy Protection, and information on the device is hidden.

➧ *To enable Privacy Protection remotely using a telephone standard tools for creating an SMS,*

send a standard SMS to another device; it should contain the text **hide:<code>** where **<code>** is the secret code of the application set on the target device. The message is not case sensitive, and spaces before or after the colon are ignored.

SELECTING DATA TO HIDE: PRIVACY PROTECTION

Privacy Protection can hide the following info for numbers in the Contact List: contacts, SMS correspondence, call log entries, incoming calls and SMS messages. You can select information and events that Privacy Protection should hide for private numbers.

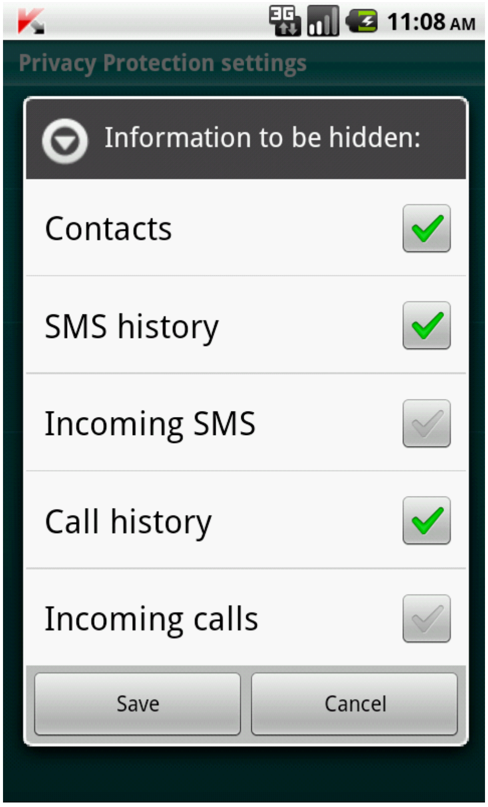
Disable Privacy Protection prior to editing Privacy Protection settings.

➧ *To select information and events that should be hidden for private numbers:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection** section.
2. Tap **Settings**.

   The **Privacy Protection settings** screen opens (see fig. below).
3. Select information and events which are hidden for confidential numbers. To do so, select **Hidden information** and check the boxes next to the required settings. The following settings are available:
   - **Contacts** – hide all information about confidential numbers in the Contacts.
   - **SMS history**—hide SMS messages in the **Incoming**, **Drafts** and **Sent** folders for confidential numbers.
   - **Incoming SMS** – hide new incoming SMS from private numbers.

- **Call history** - accept calls from confidential numbers, but do not show the caller number and do not display information about confidential numbers on the list of calls (incoming, outgoing, and missed).
- **Incoming calls** – block calls from private numbers (caller will hear the engaged tone in this case). Information about a received call will be displayed when Privacy Protection is disabled.



☑ Contacts
☑ SMS history
☐ Incoming SMS
☑ Call history
☐ Incoming calls

Figure 31. Selection of information and events to hide

CREATING A LIST OF PRIVATE NUMBERS

The contact list contains private numbers, for which Privacy Protection hides associated information and events. You can extend the list by adding a number manually, or importing one from Contacts or the SIM card.

Before making the contact list, disable hiding of confidential information.

IN THIS SECTION

ADDING A NUMBER TO THE LIST OF PRIVATE NUMBERS

You can add telephone numbers to the list of hidden contacts or import them from Contacts.

Before making the contact list, disable hiding of confidential information.

➧ *To add a phone number to the list of hidden contacts:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection** section.
2. Tap **Private Contacts**.

   The **Private Contacts** screen will appear.
3. Perform one of the following actions (see Figure below).
   - To add a number from Contacts, select **Add** → **Contact**. Select the required entry in the list of contacts on the screen.
   - To add a number manually, tap **Add** → **Number**, complete the **Phone number** field, and tap **Save**.

The number will be added to the Private Contacts list.

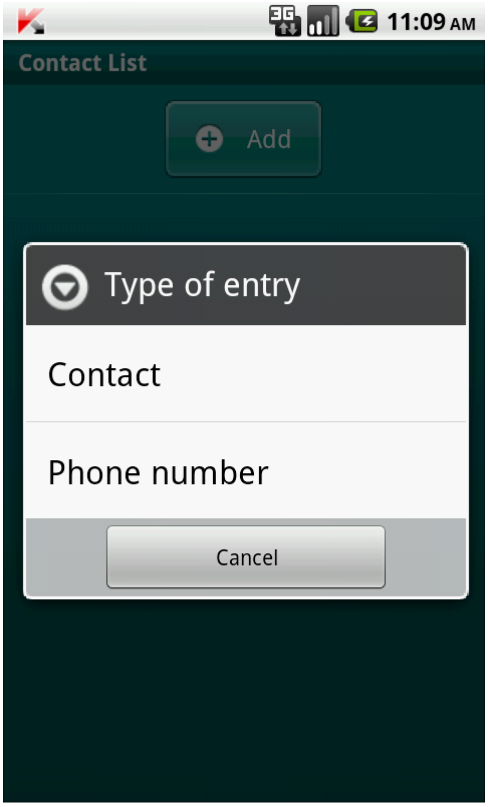


Figure 32. Adding entries to the list of protected contacts

EDITING A NUMBER IN THE LIST OF PRIVATE NUMBERS

Disable Privacy Protection prior to editing Privacy Protection settings.

The only phone numbers available for editing in the Private Contacts list are those added manually. It is not possible to edit numbers that have been selected from Contacts.

➧ *To edit a phone number on the Private Contacts list:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection** section.
2. Tap **Private Contacts**.

   The **Private Contacts** screen will appear.
3. Select the number to edit from the Private Contacts list, and select **Edit** in the context menu.

   The **Changing an entry** screen opens.
4. Edit the details.
5. Tap **Save** when the changes are complete.

The number is changed.

DELETING A NUMBER FROM THE LIST OF PRIVATE NUMBERS

You can delete one number or clear the Private Contacts list completely.

Disable Privacy Protection prior to editing Privacy Protection settings.

➧ *To remove a number from the Private Contacts list:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection** section.
2. Tap **Private Contacts**.

   The **Private Contacts** screen will appear.
3. Select the number to be deleted, and select **Delete** in the context menu.

➧ *To clear the Private Contacts list:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Privacy Protection**.
2. Tap **Private Contacts**.

   The **Private Contacts** screen will appear.
3. In the context menu, select **Delete all**.

   The confirmation window opens.
4. Confirm deletion. To do this, press **Yes**.

The Private Contacts list will become empty.

UPDATING THE APPLICATION'S DATABASES

This section provides information on updating the application databases, which ensures up-to-date protection of your device. Furthermore, this section describes how to view information on the installed anti-virus databases, run the update manually, and configure automatic update of anti-virus databases.

IN THIS SECTION

ABOUT UPDATING THE APPLICATION DATABASES

The application scans the device for malware programs using the application anti-virus database, which contains descriptions of all currently known malware and other undesirable programs, and methods for their treatment. It is extremely important to keep your anti-virus databases up-to-date.

It is recommended to regularly update the application databases. If more than 15 days have passed since the last update, the databases are regarded as obsolete. Protection will then be less reliable.

Kaspersky Endpoint Security 8 for Smartphone updates the application's database from the update servers set by the administrator.

To update the application's anti-virus databases, you must have an Internet connection configured on your mobile device.

Application anti-virus databases are updated according to the following algorithm:

1. The application databases installed on your mobile device are compared with those located on the special update server.
2. Kaspersky Endpoint Security 8 for Smartphone performs one of the following:
   - If you have the current application's databases installed, the update will be canceled. A notification appears on the screen.
   - If the installed databases differ, a new update package is downloaded and installed.

     When the update process is completed, the connection is automatically closed. If the connection was established before the update started, it will remain open for further use.

You can start the update task manually at any time when the device is not busy with other tasks or schedule automatic updates.

Detailed information about the anti-virus databases used is available in the **Anti-Virus** → **Additional** section under the **Start update** item.

STARTING UPDATES MANUALLY

You can start the application anti-virus databases update manually.

➧ *To start the anti-virus database update process manually:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Tap **Start update**.

The application starts the process of updating the databases from the Kaspersky Lab server. Information on the update process is displayed on the screen.

STARTING SCHEDULED UPDATES

Regular updates are a prerequisite of effectively protecting your device against infection by malware objects. For your convenience, you can configure automatic database updates and create an update schedule.

To run an update, the device should remain turned on for the entire scan period.

In addition, you can configure the automatic update settings for when you are in a roaming zone.

➧ *To configure a scheduled update start:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Anti-Virus** section.
2. Tap **Additional**.

   The **Anti-Virus: Additional** screen opens.
3. Select the **Automatic update** item.

   The **Automatic update** screen opens.
4. Select one of the following values for the **Scheduled update** setting:

   - **Weekly**: update application databases once a week. Select values for the **Start day** and **Start time** settings.
   - **Daily** – update the application databases every day. Enter a value for the **Start time** setting.
   - **Disabled** – do not perform a scheduled update of the application databases.

CONFIGURING ADDITIONAL SETTINGS

The section provides information about the additional capabilities of Kaspersky Endpoint Security 8 for Smartphone: how to enable / disable pop-up notifications in the application status bar, sound notifications, and the display of hints before configuring each component, how to configure the Home screen widget, and how to change the secret code of the application.

IN THIS SECTION

CHANGING THE SECRET CODE

You can change the secret code set after the first start up of the application.

➡ *To change the secret code:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.

   This will open the **Additional** window.

2. Select **Change secret code**.
3. Enter the current secret code in the **Enter secret code** field, and tap **Next**.
4. Enter the new secret code in the **Set new secret code** field, and tap **Next**.

   The code entered is automatically verified.

   If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. In order to use the code, press **Yes**. In order to create a new code, press **No**. Enter a new application secret code.

5. Re-enter the same code in the **Re-enter code** field.

   The secret code is changed.

DISPLAYING HINTS

When you configure the settings of components, Kaspersky Endpoint Security 8 for Smartphone displays by default a hint containing a brief description of the function selected. You can select to show/hide hints for Kaspersky Endpoint Security 8 for Smartphone.

➡ *To show/hide hints:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

This will open the **Additional** window.

2. Depending on the task to be completed:

   - To enable the display of hints, check the **Hints** box.
   - To disable the display of hints, uncheck the **Hints** box.

CONFIGURING SOUND NOTIFICATIONS

When the application is running, various events occur; for example, if the license expires or an infected file is detected. For the application to inform you in every such event, you can enable sound notification of the occurring event.

Kaspersky Endpoint Security 8 for Smartphone includes sound notification only according to the device's set mode.

➡ *To manage the sound notification of the application, perform the following steps:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** tab.

   This will open the **Additional** window.

2. Depending on the task to be completed:

   - To enable sound notifications, check the **Sound** box.
   - To disable sound notifications, uncheck the **Sound** box.

NOTIFICATIONS IN THE STATUS BAR

Kaspersky Endpoint Security 8 for Smartphone allows you to receive pop-up notifications in the status bar about application events; for example, if the license expires or Protection is disabled. You can enable / disable the receipt of notifications about application events in the status bar.

➡ *To manage pop-up notifications about the application:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.

   This will open the **Additional** window.

2. Depending on the task to be completed:

   - To enable pop-up notifications about the application, check the **Notifications** box.
   - To disable pop-up notifications about the application, uncheck the **Notifications** box.

USING THE HOME SCREEN WIDGET

In Kaspersky Endpoint Security 8 for Smartphone, you can use the Home screen widget (on page 25). The Home screen widget is intended for indicating the state of the application license, your device protection, as well as the whether the private data is shown or hidden.

Following installation of the application, the widget appears on the Home screen of the device automatically. You can add the widget to the Home screen, delete it, or configure the Privacy Protection status indicator in the Home screen widget (see "Privacy Protection" on page 61).

➧ *To manage the display of the Home screen widget:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.

   This will open the **Additional** window.

2. Select the **Widget** item.

   The **Home screen widget** screen opens (see fig. below).

3. Depending on the task to be completed:

   - To add the widget to the Home screen of the device, check the **Enable widget** box.
   - To delete the widget from the Home screen of the device, uncheck the **Enable widget** box.

➧ *To configure the Privacy Protection status indicator in the Home screen widget:*

1. On the Home screen of Kaspersky Endpoint Security 8 for Smartphone, open the **Additional** section.

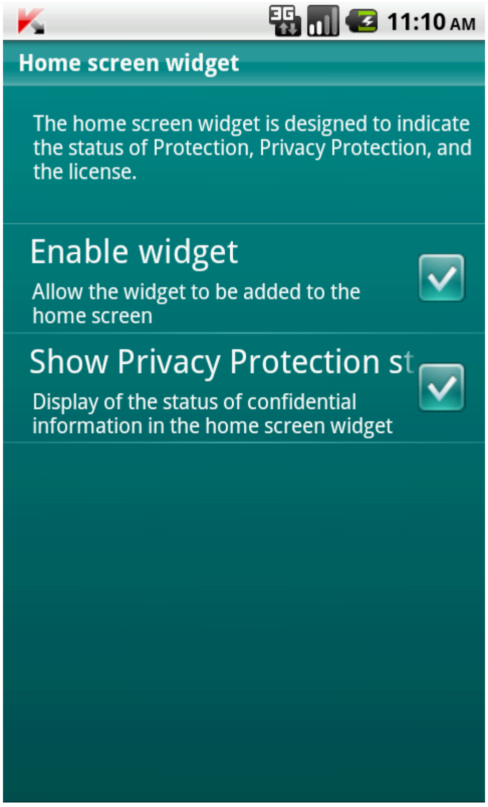
   This will open the **Additional** window.

2. Select the **Widget** item.

   The **Home screen widget** screen opens.

3. Depending on the task to be completed:

   - To display changes to the Privacy Protection mode in the Home screen widget, check the **Show Privacy Protection status** box.
   - To hide changes to the Privacy Protection mode in the Home screen widget, uncheck the **Show Privacy Protection status** box.



Home screen widget

The home screen widget is designed to indicate the status of Protection, Privacy Protection, and the license.

Enable widget ☑
Allow the widget to be added to the home screen

Show Privacy Protection st ☑
Display of the status of confidential information in the home screen widget

Figure 33. Home screen widget settings

GLOSSARY

A

ACTIVATING THE APPLICATION

Switching the application into full-function mode. Activation is carried out by the user during application installation or afterwards. To activate the application, a user needs an activation code or a key file.

ANTI-VIRUS DATABASES

Databases containing descriptions of computer security threats known to Kaspersky Lab at the time of database release. Records in the databases allow detection of malicious code in the objects being scanned. The databases are maintained by the experts of Kaspersky Lab and updated every hour.

APPLICATION SECRET CODE

The secret code prevents unauthorized access to the application settings and to blocked information on the device. The user sets it on first starting the application and it consists of at least four characters. The secret code is requested in the following instances:

- for access to application settings;
- when sending an SMS command from another mobile device to start the following functions remotely: Block, Data Wipe, SIM Watch, GPS Find, Privacy Protection.

ARCHIVE

One or multiple files packed into a single file in compressed format. Data compression and decompression require a special archiver program.

B

BLACK LIST

The list entries contain the following information:

- Phone number, from which Anti-Spam blocks calls and (or) SMS.
- Type of events invoked from the number that Anti-Spam blocks. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase that Anti-Spam uses to classify an SMS message as unsolicited (spam). Anti-Spam only blocks SMS messages containing this key phrase while delivering all the rest.

D

DELETING SMS MESSAGES

A method of processing an SMS message containing SPAM features, by deleting it. You are advised to use this method with SMS messages which definitely contain spam.

DELETION OF AN OBJECT

The method of processing objects by physically deleting it from its original location. You are advised to apply this processing method to any malicious objects which cannot be disinfected.

DISINFECTING OBJECTS

The method used for processing infected objects that results in complete or partial recovery of data, or the decision that the objects cannot be disinfected. Not all the infected objects are disinfectable.

I

INFECTED OBJECT

Object containing malicious code. The application detected infected objects by scanning their binary code, and finding that a section of the object's code is identical to a section of the code of a known threat. Kaspersky Lab's experts do not recommend using such objects since they may infect your device.

N

NON-NUMERIC NUMBER

A phone number that includes letters or consists only of letters.

P

PHONE NUMBER MASK

Including a phone number in the Black or White List using wildcards. The two basic wildcards used in phone number masks are "*" and "?", (where "*" represents any number of characters and "?" stands for any single character). For example, *1234? is in the Black List. Anti-Spam blocks calls or SMS from a number, in which any symbol follows the digits 1234.

W

WHITE LIST

The entries in this list contain the following information:

- Phone number, from which Anti-Spam delivers calls and (or) SMS.
- Type of events invoked from the number that Anti-Spam allows. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase used by Anti-Spam to classify an SMS message as solicited (not spam). Anti-Spam only delivers SMS messages containing the key phrase and blocks all others.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems — from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*; and the *Anti-Spam database every five minutes*.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab website:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com/
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending probably infected files in archive format)
	http://support.kaspersky.com/virlab/helpdesk.html
	(for sending requests to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com/

INFORMATION ABOUT THIRD-PARTY CODE

Third party code is used to create the application.

IN THIS SECTION

DISTRIBUTED PROGRAM CODE

Within the application, an independent third-party program code is distributed in source or binary form, without any changes made.

IN THIS SECTION

ADB

ADBWINAPI.DLL

ADBWINUSBAPI.DLL

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to

those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

OTHER INFORMATION

To create and verify digital signatures, Kaspersky Endpoint Security 8 for Smartphone uses Crypto C data security software library by CryptoEx LLC.

CryptoEx Ltd corporate website http://www.cryptoex.ru

TRADEMARK NOTICE (ANDROID)

Registered trade and service marks are the property of their respective owners.

Android and Google – trademarks of Google, Inc.

INDEX