

Kaspersky Mobile Security 9

for BlackBerry

The Kaspersky Lab logo is displayed diagonally across a white band. The word "KASPERSKY" is in a large, bold, dark teal font, with a small red triangle pointing left inside the letter 'A' and another small red triangle pointing right inside the letter 'S'. To the right of "KASPERSKY", the word "lab" is written in a smaller, red, lowercase font, rotated 90 degrees counter-clockwise.

User Guide

PROGRAM VERSION: 9.0

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 the 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.

In this document, registered trademarks and service trademarks are used which are the property of the corresponding rights holders.

Revision date: 24.10.2011

© 2011 Kaspersky Lab ZAO. All Rights Reserved.

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

TABLE OF CONTENTS

ABOUT THIS GUIDE	5
In this document	5
Document conventions	Error! Bookmark not defined.
ADDITIONAL DATA SOURCES	ERROR! BOOKMARK NOT DEFINED.
Information sources for further research.....	Error! Bookmark not defined.
Contacting the Sales Department.....	Error! Bookmark not defined.
Discussion of Kaspersky Lab applications on the Web forum	Error! Bookmark not defined.
Contacting the Documentation Development Group	Error! Bookmark not defined.
KASPERSKY MOBILE SECURITY 9	11
Distribution kit.....	11
Hardware and software requirements.....	12
INSTALLING KASPERSKY MOBILE SECURITY 9	13
UNINSTALLING THE APPLICATION	18
GETTING STARTED.....	ERROR! BOOKMARK NOT DEFINED.
Activating the application.....	14
Activating the commercial version.....	15
Activating the subscription for Kaspersky Mobile Security 9	15
Purchasing an activation code online.....	16
Activating the trial version	17
Setting the secret code.....	17
Enabling the option to recover the secret code.....	18
Recovering the secret code	27
Starting the application	26
Viewing information about the application	19
MANAGING THE LICENSE	ERROR! BOOKMARK NOT DEFINED.
About the License Agreement	Error! Bookmark not defined.
About Kaspersky Mobile Security 9 licenses	Error! Bookmark not defined.
View License Information.....	22
Renewing the license	22
Renewing the license with the activation code.....	23
Renewing the license online	23
Renewing the license by activating the subscription	23
Unsubscribing	24
Renewing the subscription	24
APPLICATION INTERFACE	28
Application menu	28
Protection status window	28
FILTERING OF INCOMING CALLS AND SMS.....	30
About Call&SMS Filter	30
About Call&SMS Filter modes	30
Changing the Call&SMS Filter mode	31
Creating the Black List.....	31

Adding entries to the Black List	32
Editing entries in the Black List	33
Deleting entries from the Black List.....	34
Creating a White List	34
Adding entries to the White List	35
Editing entries in the White List.....	36
Deleting entries from the White List	36
Responding to SMS messages and calls from contacts not in the phone book.....	37
Responding to SMS messages from non-numeric numbers.....	38
Selecting a response to incoming SMS	38
Selecting response to incoming calls.....	39
DATA PROTECTION IN THE EVENT OF LOSS OR THEFT OF THE DEVICE	40
About Anti-Theft.....	40
Blocking the device.....	41
Deleting personal data.....	42
Creating a list of folders to delete	44
Monitoring the replacement of a SIM card on the device.....	45
Determining the device's geographical coordinates.....	46
Starting Anti-Theft functions remotely.....	47
APPLICATION LOGS.....	49
About logs.....	49
Viewing Log records	49
Deleting Log records	49
CONFIGURING ADDITIONAL SETTINGS	50
Changing the secret code.....	50
Displaying prompts	50
CONTACTING THE TECHNICAL SUPPORT SERVICE	ERROR! BOOKMARK NOT DEFINED.
GLOSSARY	54
KASPERSKY LAB.....	56
INFORMATION ABOUT THIRD PARTY CODE.....	57
Distributed program code	57
ADB	57
ADBWINAPI.DLL	57
ADBWINUSBAPI.DLL.....	57
Other information.....	59
INDEX	60

ABOUT THIS GUIDE

This document is the Kaspersky Mobile Security User Guide.

For efficient use of Kaspersky Mobile Security users should have basic skills of handling their mobile device: they should be familiar with the interface of the operating system that they use, be aware of basic working methods, and know how to use email and Internet.

This guide is intended to:

- Help you install, activate, and use Kaspersky Mobile Security.
- Ensure a quick search of information on issues related to Kaspersky Mobile Security operation.
- Describe additional sources of information about the application and ways of cooperating with the Technical Support Service.

IN THIS SECTION

In this document.....	5
Document conventions.....	7

IN THIS DOCUMENT

The following sections are included in the document:

Additional data sources

This section describes additional sources of information about the application and Internet resources, on which users can discuss the application, ask questions, and get answers.

Kaspersky Mobile Security 9

This section describes the application's features and provides a brief overview of its components and main functions. This section provides information about the purpose of the distribution kit. This section lists hardware and software requirements that a mobile device should meet to allow installation of Kaspersky Mobile Security 9.

Installing Kaspersky Mobile Security 9

This section contains instructions that can help you install the application on a mobile device.

Uninstalling the application

This section contains instructions that can help you uninstall the application from a mobile device.

Updating the application

This section contains instructions that can help you update the previous version of the application.

Getting started

This section provides information about how to start working with Kaspersky Mobile Security 9: activate it, set a secret code for the application, enable the option of secret code recovery, recover the secret code, start the application, update anti-virus databases, and scan a device for viruses.

Managing the license

This section contains information about common terms used in the framework of the application licensing. Furthermore, the section presents information about how to find information on the Kaspersky Mobile Security 9 license and extend the term of its validity.

Application interface

This section includes information on the main elements of the Kaspersky Mobile Security 9 interface.

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.

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.

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.

Filtering of incoming calls and SMS

This section gives information about Call&SMS Filter which prevents unwanted calls and SMS according to the Black and White Lists you create. The section also describes how to select the mode in which Call&SMS Filter scans incoming calls and SMS, how to configure additional filtering settings for incoming SMS and calls and also how to create Black and White Lists.

Restricting outgoing calls and SMS messages. Parental Control

The section presents information on the Parental Control component, which allows limiting outgoing calls and SMS messages to defined numbers. Furthermore, the section describes how to create a list of allowed and banned numbers and set the Parental Control settings.

Data protection in the event of loss or theft of the device

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 the parameters of its operation and start Anti-Theft from another mobile device remotely.

Privacy Protection

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

Filtering network activity. Firewall

This section gives information about the Firewall which controls network connections on your device. This section describes how to enable/disable the Firewall and select the required mode for it.

Encrypting personal data

This section gives information about Encryption, which can encrypt folders on the device. It also describes how to encrypt and decrypt selected folders.

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.

Application logs

This section presents information on logs which register the operation of every component and the execution of every task (e.g. application database updates, virus scans).

Configuring additional settings

This section provides information on additional options of Kaspersky Mobile Security 9: how to manage the application's sound notification and screen backlight and how to enable/disable the display of the hints, protection icon and protection status window.

Contacting the Technical Support Service

This section contains recommendations for contacting Kaspersky Lab for help from your Personal Cabinet on the Technical Support Service website or by phone.

Glossary

This section contains a list of terms used within the document and their respective definitions.

Kaspersky Lab

The section provides information on Kaspersky Lab ZAO.

Information about third party code

This section gives you information on third-party code used in the application.

Index

This section enables you to quickly find the required information in the document.

DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Note that...	Warnings are highlighted with red color and boxed. Warnings provide information about probable unwanted actions that may lead to data loss or failures in computer operation.
It is recommended to use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values, or important particular cases in the application's operation.
Example: ...	Examples are set out on a yellow background under the heading "Example".
Update means... The <i>Databases are out of date</i> event occurs.	The following semantic elements are italicized in the text: <ul style="list-style-type: none"> new terms; names of application statuses and events.
Press ENTER on the keyboard. Press ALT+F4 .	Names of keyboard keys appear in a bold typeface and are capitalized. Names of keys connected by a + (plus) sign indicate the use of a key combination. Those keys should be pressed simultaneously.
Click the Enable button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and accompanied by the arrow sign.
Enter <code>help</code> in the command line. The following message then appears: Specify the date in dd:mm:yy format.	The following types of text content are set off with a special font: <ul style="list-style-type: none"> text in the command line; text of messages displayed on the screen by the application; data that the user should enter.
<IP address of your mobile device>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

SOURCES OF INFORMATION ABOUT THE APPLICATION

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

IN THIS SECTION

Information sources for further research	9
Contacting the Sales Department	Error! Bookmark not defined.
Discussion of Kaspersky Lab applications on the Web forum	Error! Bookmark not defined.
Contacting the Documentation Development Group	Error! Bookmark not defined.

INFORMATION SOURCES FOR FURTHER RESEARCH

You can use the following sources to find information about the application:

- the application page on the Kaspersky Lab website;
- the application page on the Technical Support Service website (Knowledge Base);
- online help;
- documentation.

If you cannot solve an issue on your own, we recommend that you contact the Technical Support Service at Kaspersky Lab (see section "Technical support by phone" on page [51](#)).

To use information sources on the Kaspersky Lab website, an Internet connection should be established.

Page on Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

On such a page (http://www.kaspersky.com/kaspersky_mobile_security), you can view general information about an application, its functions and features.

The page <http://www.kaspersky.com> features a URL to the eStore. There you can purchase or renew the application.

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

Knowledge Base is a section of the Technical Support Service website that provides recommendations on how to work with Kaspersky Lab applications. Knowledge Base comprises reference articles grouped by topics.

On the page of the application in the Knowledge Base you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Articles may provide answers to questions that are out of scope of Kaspersky Mobile Security, being related to other Kaspersky Lab applications. They also may contain news from the Technical Support Service.

Online help

The online help of the application comprises context help files.

The context help contains data on each of the windows and tabs in Kaspersky Mobile Security: a list of settings and their respective descriptions, as well as a list of tasks to perform.

The installed Documentation

The application user guide provides information about how to install, activate, and configure the application, as well as application operation data. The document describes the application interface and the capabilities offered for typical application tasks.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab specialists and other users on our Forum (<http://forum.kaspersky.com>).

In this forum you can view existing topics, leave your comments, create new topics.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our HQ office in Moscow by phone (<http://www.kaspersky.com/contacts>).
- By sending a message with your question by email.

The service is provided in Russian or English.

CONTACTING THE DOCUMENTATION DEVELOPMENT TEAM BY EMAIL

To contact the Documentation Development Team, send an email. Please use "Kaspersky Help Feedback: Kaspersky Internet Security" as the subject line in your message.

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 protects mobile devices running BlackBerry OS operating system. The application controls incoming SMS and calls and protects information on the device in case of theft or loss. 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 Mobile Security 9 includes the following protection components:

- **Call&SMS Filter.** Scans all incoming SMS messages and calls for spam. The component allows the flexible blocking of text messages and calls considered undesirable.
- **Anti-Theft.** 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 (if your mobile device has a GPS receiver) 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.

Besides, the application contains a set of service features. These increase the application's possible uses, as well as helping the user in their work:

- **Protection status.** The status of the program's components is displayed on screen. Based on the information presented, you can evaluate the current information protection status on your device.
- **Events log.** Each of the program's components has its own events log, which contains information about the component's operations (e.g. remote launch of the Anti-Theft function, status of the program's license validity period).
- **Uninstalling the application.** To prevent access to protected information, Kaspersky Mobile Security 9 can only be uninstalled from the application's interface.

Kaspersky Mobile Security 9 is not intended for backup and restore.

IN THIS SECTION

Distribution kit.....	11
Hardware and software requirements	12

DISTRIBUTION KIT

You can purchase Kaspersky Mobile Security 9 online, in which case the application's distribution kit and documentation are provided in electronic form. Kaspersky Mobile Security 9 can be also purchased from all good phone and technology retail stores. For detailed information about purchasing the application and receiving the distribution kit, please contact our sales department at sales@kaspersky.com.

SERVICE FOR REGISTERED USERS

On purchasing a user license for the application, you become a registered user of Kaspersky Lab applications and can benefit from the following services during the entire validity term of the license:

- updating databases and providing new versions of the application;
- consulting by phone and by email on issues related to installation, configuration, and use of the application;

- notifying you of releases of new applications by Kaspersky Lab and new viruses. To use this service, you should be subscribed to the news delivery from Kaspersky Lab on the Technical Support Service website.

No consulting services are provided on issues related to the functioning of operating systems, third-party software and technologies.

HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Mobile Security 9 can be installed on mobile devices using the BlackBerry OS 4.5, 4.6, 4.7, 5.0 and 6.0 operating systems.

INSTALLING AND REMOVING THE APPLICATION

This section provides information about how to install the application on a mobile device and how to uninstall it.

IN THIS SECTION

Installing Kaspersky Mobile Security 9.....	Error! Bookmark not defined.
Activating the application.....	Error! Bookmark not defined.
Setting the secret code.....	Error! Bookmark not defined.
Enabling the option to recover the secret code	Error! Bookmark not defined.
Uninstalling the application.....	Error! Bookmark not defined.

INSTALLING KASPERSKY MOBILE SECURITY 9

The application is installed on a mobile device in several steps.

To install Kaspersky Mobile Security 9, an Internet connection should be configured on the device.

➡ To install Kaspersky Mobile Security 9:

1. Perform one of the following actions:

- If you have purchased the program on a CD, connect the mobile device to the computer using the BlackBerry Desktop Manager and run the automatic Kaspersky Mobile Security 9 installation on the CD purchased.

Installation is only possible if Blackberry Desktop Manager is installed on the computer.

- If you have purchased the distribution package on the Internet, perform one of the following actions on the mobile device:
 - Open the message with the link to the distribution package, follow the link and download the application distribution package to the mobile device;
 - Download the application distribution package at Kaspersky Lab eStore.

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

If you have purchased the distribution package on the Internet, you can only install the application through the mobile device itself. In this case, installation of Kaspersky Mobile Security 9 through a computer is not supported.

2. Run the application. To do this, select **Menu** → **Download** → **KMS 9** and launch the application by using the scroll bar or selecting **Menu** → **Open**.

3. Set the application secret code. To this end, fill in the **Enter new code** and **Confirm code** fields and press **ENTER**.

ACTIVATING THE APPLICATION

Before starting to use Kaspersky Mobile Security 9, it needs to be activated.

To activate Kaspersky Mobile Security 9 on your device, you must have an Internet connection configured.

Before activating the application, make sure that the device's system date and time settings are correct.

You can activate the application as follows:

- **Activate trial license.** When you activate the trial version, the application receives a free trial license. The validity period of the trial license is displayed on the screen after the activation is complete. Once the validity period of the trial license expires, the application's functions will be limited. The following features will only be available:

- Activating the application;
- managing the application license;
- Kaspersky Mobile Security 9 Help system;

It is impossible to reactivate a trial version.

- **Activate commercial license.** To activate the commercial version, you should use the activation code that you have received when purchasing the application. When activating the commercial version, the application receives a commercial license, which grants you access to all the application's functions. The license validity period is displayed on the screen of the device. Once the validity period of the trial license expires, the application's functions will be limited.

You can obtain an activation code as follows:

- online, by going from the Kaspersky Mobile Security 9 application to the special Kaspersky Lab website for mobile devices;
 - at Kaspersky Lab eStore (<http://www.kaspersky.com/globalstore>);
 - from Kaspersky Lab distributors.
- **Activate subscription.** When activating the subscription, the application receives a commercial license with subscription. The validity period of the commercial license with subscription is limited to 30 days. When the subscription is activated, the application renews the license each 30 days. When the license is renewed, a fixed payment for application use specified at the subscription activation, is written off from your personal account. The funds are debited by sending a payable SMS message. Once the funds are debited, the application receives a new license from the activation server, with a subscription which grants access to all functions of the application. You can cancel the subscription for Kaspersky Mobile Security 9. In this case, when the current license expires, the application's functionality becomes limited.

IN THIS SECTION

Activating the commercial version	15
Activating the subscription for Kaspersky Mobile Security 9	15
Purchasing an activation code online	16
Activating the trial version	17

ACTIVATING THE COMMERCIAL VERSION

➤ *To activate the commercial version of the application with the activation code:*

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 9**.

The application installation folder may vary depending on the mobile device model.

3. Start the application. To do this, use the scroll bar or select **Menu** → **Open**.
4. Select **Enter activation code**.

The Kaspersky Mobile Security 9 activation window opens.

5. Enter the activation code that you have received when purchasing the application and press **Activate**.
6. Confirm the connection to the Internet by pressing **Yes**.

The application will send a request to the Kaspersky Lab activation server and receive a license. When the license is successfully received, information about it will be displayed on the screen.

If the activation code you entered is invalid for any reason, an information message is displayed on the screen. In such a case, we recommend checking that the entered activation code is correct and contact the software vendor you have purchased Kaspersky Mobile Security 9 from.

If any errors have occurred when connecting to the server and no license has been received, the activation is canceled. In this event, it is recommended verifying the parameters of connecting to the Internet. If it was not possible to rectify the errors, contact Technical Support.

7. Go to setting the application secret code.

ACTIVATING THE SUBSCRIPTION FOR KASPERSKY MOBILE SECURITY 9

To activate the subscription, an Internet connection should be established on the device.

➤ *To activate the subscription for Kaspersky Mobile Security 9:*

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 9**.

The application installation folder may vary depending on the mobile device model.

Start the application. To do this, use the scroll bar or select **Menu** → **Open**.

3. Select **One-Click Buy**.
4. Confirm the connection to the Internet by pressing **Yes**.

The application will check if the subscription service is accessible to the mobile service provider that you use. If the subscription service is available, the **Activation** screen opens, displaying information about the terms of subscription.

If the subscription service cannot be provided, the application will notify you of this and switch back to the screen on which you can select another way of activating the application.

5. Read through the terms of subscription and then confirm the activation of subscription for Kaspersky Mobile Security 9 by pressing **Activate**.

The application will send a payable SMS and then receive a license from the activation server of Kaspersky Lab. When the subscription becomes activated, Kaspersky Mobile Security 9 will notify you of this.

If your balance has not enough funds to send a payable SMS message, the subscription activation will be canceled.

If any errors have occurred when connecting to the server and no license has been received, the activation is canceled. In this event, it is recommended verifying the parameters of connecting to the Internet. If it was not possible to rectify the errors, contact Technical Support.

If you do not agree the terms of subscription, press **Cancel**. In this case, the application cancels the subscription activation and goes back to the screen in which you can reselect the way of activating the application.

6. On completing the activation go to setting the secret code.

PURCHASING AN ACTIVATION CODE ONLINE

➡ In order to purchase an activation code for the application online, perform the following steps:

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 9**.

The application installation folder may vary depending on the mobile device model.

Start the application. To do this, use the scroll bar or select **Menu** → **Open**.

3. Select **Buy online**.

This will open the **Buy online** window.

4. Press **Open**.

A special Kaspersky Lab website for mobile devices opens, on which you will be offered to order the license renewal.

5. Follow the step-by-step instructions.
6. After you are done with purchasing an activation code, proceed with (see section "Activating the commercial version" on page [15](#)).

ACTIVATING THE TRIAL VERSION

➡ To activate the trial version of Kaspersky Mobile Security 9:

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 9**.

The application installation folder may vary depending on the mobile device model.

Start the application. To do this, use the scroll bar or select **Menu** → **Open**.

3. Select **Trial version**.
4. Confirm the connection to the Internet by pressing **Yes**.

The application will send a request to the Kaspersky Lab activation server and receive a license.

If any errors have occurred when connecting to the server and no license has been received, the activation is canceled. In this event, it is recommended verifying the parameters of connecting to the Internet. If it was not possible to rectify the errors, contact Technical Support.

5. Go to setting the application secret code.

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 Mobile Security 9 requests the secret code in the following circumstances:

- 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.

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 [19](#)). For this purpose, the recovery of secret code option must be enabled in advance (see the "Enabling the option to recover the secret code" section on page [18](#)).

➡ To enter the secret code:

1. Confirm that you wish to create an application secret code. To do this, after the application first launches, press **OK**.
The screen for entering the application secret code opens.
2. Enter the figures that will form your code in the **Enter new code** field.
3. Re-enter the same code in the **Confirm code** field.
4. Press **ENTER** on the keyboard.

The code entered is automatically verified.

If the secret code entered is valid, the protection status window opens.

If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. To use the code, press Yes.

In order to create a new code, press **No**. The **Enter new code** and **Confirm code** fields will empty. Enter a new application secret code.

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 Mobile Security 9 on the device.

You can only recover the application secret code (see the "Recovering the secret code" section on page [19](#)) 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 Mobile Security 9.

➡ 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 [17](#)) 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 clicking **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.

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 Mobile Security 9:

1. Disable hiding of confidential information.
2. Uninstall Kaspersky Mobile Security 9. To do this, select **Delete application** on the **Additional** tab (see Figure below).

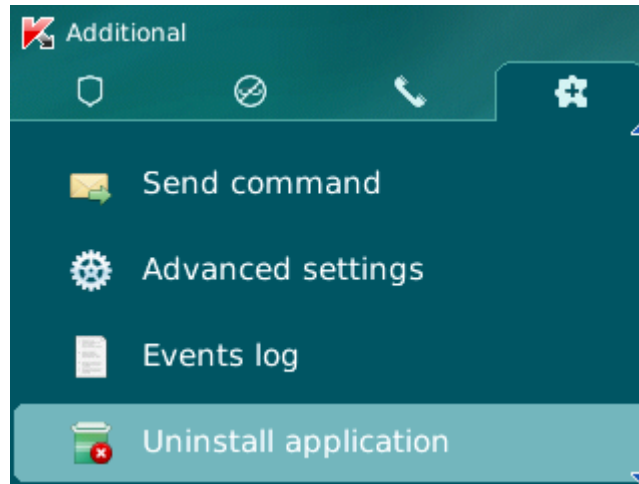


Figure 1. Uninstalling the application

A confirm deletion window opens.

3. Confirm the deletion of Kaspersky Mobile Security 9 by pressing the **Yes** button.

The deletion of the application begins.

4. Restart the device in order to complete the uninstalling of the application.

LICENSING THE APPLICATION

This section provides information about general terms related to the application activation. Read this section to learn more about the purpose of the license agreement, license types, ways of activating the application, and the license renewal.

IN THIS SECTION

About the License Agreement	20
About Kaspersky Mobile Security 9 licenses	Error! Bookmark not defined.
View License Information	22
Renewing the license	22

ABOUT THE END USER LICENSE AGREEMENT

License Agreement is a legal agreement concluded between you and Kaspersky Lab ZAO that stipulates the terms of use for the application.

Read through the terms of the License Agreement carefully before you start using the application.

You can read through the terms of the License Agreement when installing the Kaspersky Lab application.

The terms of the License Agreement are regarded as accepted in the following cases:

- Upon unsealing the box with the setup CD (only if you have purchased the application in the boxed version or at a store of any of our partners).
- Upon confirming your acceptance of the text of the License Agreement when installing the application.

If you do not accept the terms of the License Agreement, you have to interrupt the application installation.

ABOUT LICENSE

License is a time-limited right to use the application provided to you in accordance with the License Agreement. The license contains a unique code for the activation of your copy of Kaspersky Mobile Security.

The license grants you the right to benefit the following services:

- Using the application on one or several devices.

Number of devices, on which you can use the application, is specified in the License Agreement.

- Contacting the Technical Support Service of Kaspersky Lab.
- Enjoying the complete set of services provided to you by Kaspersky Lab or its partners during the validity term of the license (see section "Service for registered users" on page [Error! Bookmark not defined.](#)).

The scope of services provided and the validity term of the application depend on the type of license used to activate the application.

The following license types are available:

- *Trial* – a free license with a limited validity period, offered to allow you to become familiar with the application.

As soon as the trial license expires, all Kaspersky Mobile Security features become disabled. To continue using the application, you should purchase the commercial license.

- *Commercial* – a paid license with a limited validity period, offered upon purchase of the application.

When the commercial license expires, the application keeps running but its functionality becomes limited. You will still be able to scan your mobile device for viruses and use other application components but only with databases installed before the license has expired. To continue using Kaspersky Mobile Security in full-functional mode, you should renew the commercial license.

We recommend that you renew the license on the day the current license expires at the latest in order to ensure the most comprehensive anti-virus protection of your mobile device.

- *Commercial with activated One-click buy option* – paid license with an option of renewal in automatic or manual mode. A license with activated One-click buy option is distributed by service providers.

The license with activated One-click buy option is valid for a limited period (30 days). After the license expires, it can be extended manually or automatically. Method of extending the license depends on the legislation and mobile service provider. The license with activated One-click option is extended automatically subject to timely prepayment to the provider.

When extending the license with the activated One-click buy option, the fixed amount specified in the One-click buy terms is written off from your personal account. Funds are debited from your personal account after you send a payable SMS message to the number of the service provider.

If the license is not extended, Kaspersky Mobile Security 9 stops updating the application databases, and the application's functionality becomes limited.

When using the license with activated One-click buy option, you can activate the commercial license with an activation code. In this case, the One-click buy activation will be canceled automatically.

When using the commercial license, you can activate One-click buy. If already have an activated license with a limited term at the time of One-click buy activation, it is substituted with the license with activated One-click buy option.

ABOUT THE ACTIVATION CODE

Activation code is a code that you receive on purchasing the commercial license for Kaspersky Mobile Security. This code is required for activation of the application.

The activation code is an alphanumeric string of Latin characters in xxxxx-xxxxx-xxxxx-xxxxx format.

Depending on the way of purchasing the application, the following options are available for receiving an activation code:

- If you have purchased the boxed version of Kaspersky Mobile Security, the activation code is specified in the documentation or on the box containing the setup CD.
- If you have purchased Kaspersky Mobile Security at an online store, the activation code is sent to the email address that you have specified when ordering the product.

The validity term of the license starts from the moment you have activated the application. If you have purchased a license intended for the use of Kaspersky Mobile Security on several devices, the validity term of the license starts counting down from the moment you have entered the code on the first of those devices.

If you have lost or accidentally deleted your activation code after the activation, you should send a request to the Technical Support Service at Kaspersky Lab from My Kaspersky Account (see section "Obtaining technical support via My Kaspersky Account" on page [52](#)).

On completion of the application activation with a code, you are assigned a *client ID*. Client ID is the personal ID for a user, that is needed for receiving technical support by phone or via My Kaspersky Account (see section "Obtaining technical support via My Kaspersky Account" on page [52](#)).

VIEW 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. Select the **Additional** tab.
2. Select the item **License** → **About license**.

This will open the **About license** window.

RENEWING THE LICENSE

Kaspersky Mobile Security 9 allows you to renew the application license.

The license can be extended in one of the following ways:

- Enter activation code - activate the application with the activation code. You can purchase the activation code at <http://www.kaspersky.com/globalstore>, or from your local Kaspersky Lab distributor.
- Buy activation code online – go to the website visited from your mobile device, and purchase an activation code online.
- Subscribe for Kaspersky Mobile Security 9 – activate the subscription in order to renew the license each 30 days.

To activate the application on your mobile device, you must have an Internet connection configured.

IN THIS SECTION

Renewing the license with the activation code	23
Renewing the license online.....	23
Renewing the license by activating the subscription	23
Unsubscribing	24
Renewing the subscription	24

RENEWING THE LICENSE WITH THE ACTIVATION CODE

➡ *To renew the license with the activation code:*

1. Open the **Additional** tab.
2. Select the item **License** → **Enter activation code**.

This will open the **Activation** window.
3. Enter the activation code obtained in four fields and then select **Next**.
4. Confirm establishing Internet connection by pressing **Yes**.

The application will send a request to the Kaspersky Lab activation server and receive a license. When the license is successfully received, information about it will be displayed on the screen.

If the activation code you entered is invalid for any reason, an information message is displayed on the screen. In such a case, we recommend checking that the entered activation code is correct and contact the software vendor you have purchased Kaspersky Mobile Security 9 from.

If any errors have occurred when connecting to the server and no license has been received, the activation is canceled. In this event, it is recommended verifying the parameters of connecting to the Internet. If it was not possible to rectify the errors, contact Technical Support.

5. On completion, press **OK**.

RENEWING THE LICENSE ONLINE

➡ *To renew your license online:*

1. Select the **Additional** tab.
2. Select the item **License** → **Buy online**.

This will open the **Buy online** window.

3. Press **Open**.

A website opens, which offers you to order the license renewal.

If the license has expired, a special Kaspersky Lab website for mobile devices opens on which you can buy an activation code online.

4. Follow the step-by-step instructions.
5. When the order to renew the license is processed, enter the activation code obtained (see the "License renewal with activation code" section on page [23](#)).

RENEWING THE LICENSE BY ACTIVATING THE SUBSCRIPTION

In the Additional menu, you can extend the license validity term by activating the subscription (see the "About Kaspersky Mobile Security 9 licenses" section on page [Error! Bookmark not defined.](#)) for Kaspersky Mobile Security 9. When the subscription is activated, Kaspersky Mobile Security 9 renews the license each 30 days. Every time the license is renewed, the fixed amount specified in the terms of subscription is debited from your personal account.

To activate the subscription for Kaspersky Mobile Security 9 on your device, you should have an Internet connection established.

➡ *To activate the subscription for Kaspersky Mobile Security 9:*

1. Open the **Additional** tab.

Select the item **License** → **One-Click Buy**.

2. Confirm the connection to the Internet by pressing **Yes**.

The application will check if the subscription service is accessible to the mobile service provider that you use.

If the subscription service is available, the **Activation** screen opens, displaying information about the terms of subscription.

If the subscription service cannot be provided, the application will inform you of this event and switch back to the screen on which you can select another method of renewing the license. The subscription activation will be canceled.

3. Read through the terms of subscription and then confirm the activation of subscription for Kaspersky Mobile Security 9 by pressing **Next**.

The application will send a payable SMS and then receive a license from the activation server of Kaspersky Lab. When the subscription becomes activated, Kaspersky Mobile Security 9 will notify you of this.

If your balance has not enough funds to send a payable SMS message, the subscription activation will be canceled.

If any errors have occurred when connecting to the server and no license has been received, the activation is canceled. In this event, it is recommended verifying the parameters of connecting to the Internet. If it was not possible to rectify the errors, contact Technical Support.

If you do not agree the terms of subscription, press **Cancel**. In this case, the application will cancel the subscription activation and switch back to the screen on which you can select another method of renewing the license.

4. On completion, press **OK**.

UNSUBSCRIBING

You can cancel the subscription for Kaspersky Mobile Security 9. In this case, Kaspersky Mobile Security 9 will not renew the license each 30 days. When the current license expires, the application's functionality becomes limited, and the application databases are no longer updated.

If you have canceled your subscription, you can resume it (see section "Renewing the subscription" on page [24](#)).

➡ *To unsubscribe for Kaspersky Mobile Security 9:*

1. Select the **Additional** tab.
2. Select the item **License** → **Unsubscribe**.
3. Confirm the subscription cancellation by pressing **Yes**.

Kaspersky Mobile Security 9 will notify you of cancellation of the subscription.

RENEWING THE SUBSCRIPTION

If you have canceled the subscription, you can resume it. In this case, Kaspersky Mobile Security 9 will renew the license every 30 days.

When resuming the subscription, funds are only debited from your personal account if the current license expires sooner than in three days.

➡ *To resume the subscription:*

1. Open the **Additional** tab.
2. Select the item **License** → **One-Click Buy**.

If your current license has expired, Kaspersky Mobile Security 9 will offer you to activate the subscription again (see section "Renewing the license by activating the subscription" on page [23](#)).

If the current license has not expired yet, Kaspersky Mobile Security 9 resumes the subscription and renews it each 30 days after the current license expires.

STARTING THE APPLICATION

➡ To start Kaspersky Mobile Security 9:

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 9**.

The application installation folder may vary depending on the mobile device model.

3. Start the application. To do this, use the scroll bar or select **Menu** → **Open**.
4. Enter the secret code of the application and press **OK**.

The application displays a window showing the current status of Kaspersky Mobile Security 9.

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 [18](#)).

➡ To recover the application secret code:

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 9**.

The application installation folder may vary depending on the mobile device model.

Start the application. To do this, use the scroll bar or select **Menu** → **Open**.

3. Press **Menu** → **Secret code recovery**.

The following information will then be displayed on the screen:

- Kaspersky Lab website for recovery of secret code;
- device identification code.

4. Press **Go**.

The website <http://mobile.kaspersky.com/recover-code> opens to recover the secret code.

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. Go to **Kaspersky Mobile Security 9** screen.
7. Press **Menu** → **Enter recovery code** and enter the recovery code that you have received.
8. Enter the new application secret code. To do this, enter a new application secret code in the field **Enter new code** and **Confirm code**.
9. Press **ENTER** on the keyboard.

The code entered is automatically verified.

If the secret code entered is valid, the protection status window opens.

If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. To use the code, press **Yes**.

In order to create a new code, press **No**. The **Enter new code** and **Confirm code** fields will empty. Enter a new application secret code.

APPLICATION INTERFACE

This section includes information on the main elements of the Kaspersky Mobile Security 9 interface.

IN THIS SECTION

Application menu.....	28
Protection status window.....	28

APPLICATION MENU

The application components are arranged logically and are accessible on the application tabs. Every tab ensures access to the settings of the component selected and its tasks.

The Kaspersky Mobile Security 9 menu contains the following tabs:

- **Protection status** – shows the status of all application components.
- **Anti-Theft** – protection of information on the device in the event of theft or loss.
- **Call&SMS Filter** – filtering of unwanted incoming calls and SMS.
- **Additional** – general application settings, start of synchronization of the device with the remote administration system, uninstalling the application, information about application and license.

You can switch between tabs by using the scroll bar.

PROTECTION STATUS WINDOW

The status of the main application components is displayed in the protection status window (see Figure below).

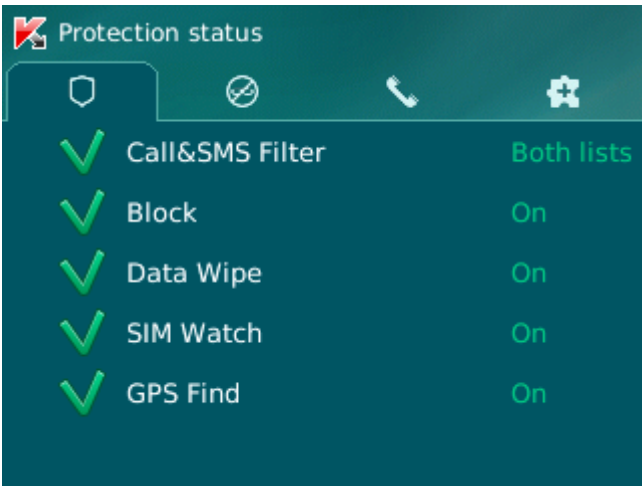


Figure 2. Current status window

The status window is immediately accessible after starting the application and contains the following information:

- **Call&SMS Filter** – mode for checking calls and SMS (see the "Filtering of incoming calls and SMS" section on page [30](#)).
- **Block, Data Wipe, SIM Watch, GPS Find** represent the Anti-Theft status (see Section "Data protection in the event of loss or theft of the device" on page [40](#)).

The **On** status means that the Anti-Theft function is enabled. The **Off** status means that the **Anti-Theft** function is disabled.

The protection status window is displayed when the application launches. You can also go to the protection status window by selecting the **Protection status** tab.

FILTERING OF INCOMING CALLS AND SMS

This section gives information about Call&SMS Filter which prevents unwanted calls and SMS according to the Black and White Lists you create. The section also describes how to select the mode in which Call&SMS Filter scans incoming calls and SMS, how to configure additional filtering settings for incoming SMS and calls and also how to create Black and White Lists.

IN THIS SECTION

About Call&SMS Filter.....	30
About Call&SMS Filter modes.....	30
Changing the Call&SMS Filter mode.....	31
Creating the Black List	31
Creating a White List	34
Responding to SMS messages and calls from contacts not in the phone book	37
Responding to SMS messages from non-numeric numbers	38
Selecting a response to incoming SMS.....	38
Selecting response to incoming calls	39

ABOUT CALL&SMS FILTER

Call&SMS Filter prevents unwanted calls and SMS to be delivered based on the Black List and White List that you have compiled.

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

- The telephone number, from which Call&SMS Filter blocks any information if the number is on the Black List and delivers any information if the number is on the White List.
- The type of event that Call&SMS Filter blocks if it is on the Black List and delivers if it is on the White List. The following types of communications are available: calls and SMS, calls only, and SMS only.
- The key phrase used by Call&SMS Filter to identify wanted and unwanted SMS. For the Black List, Call&SMS Filter blocks SMS, which contain this phrase, while delivering the ones, which do not contain it. For the White List, Call&SMS Filter delivers SMS, which contain this phrase, while blocking the ones, which do not contain it.

Anti-Spam filters calls and messages as prescribed by the selected mode (see the "About Call&SMS Filter modes" section on page [30](#)). According to the mode, Call&SMS Filter scans every incoming SMS or call and then determines whether this SMS or call is wanted or unwanted (spam). As soon as Call&SMS Filter assigns the wanted or unwanted status to an SMS or call, the scan is finished.

Information about blocked SMS and calls is registered in the application's log (see section "Application logs" on page [49](#)).

ABOUT CALL&SMS FILTER MODES

The mode defines the rules according to which Call&SMS Filter filters incoming calls and SMS.

The following Call&SMS Filter modes are available:

- **Off** – all incoming calls and SMS are allowed.
- **Black List** – all calls and SMS are allowed except those originating from numbers on the Black List.
- **White List** – only calls and SMS originating from numbers on the White List are allowed.
- **Both lists** – incoming calls and SMS from White List numbers are allowed while those from Black List numbers are blocked. Following a conversation with or the reading of an SMS from a number on neither list, Call&SMS Filter will prompt you to enter the number in either one of the lists.

You can change the Call&SMS Filter mode (see the "Changing the Call&SMS Filter mode" section on page [31](#)). The current Call&SMS Filter mode is displayed on the **Call&SMS Filter** tab next to the item **Mode**.

CHANGING THE CALL&SMS FILTER MODE

➡ To change the mode of Call&SMS Filter:

1. On the **Call&SMS Filter** tab, select the menu item **Mode**.

The **Call&SMS Filter** opens.

2. Select the value for the setting **Call&SMS Filter mode** (see figure above).

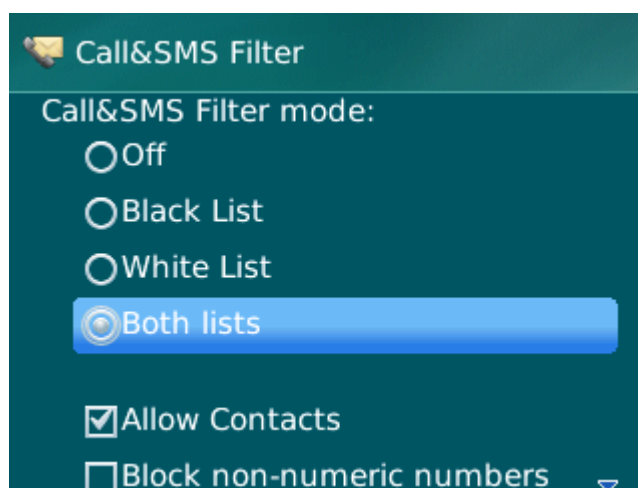


Figure 3. Changing the Call&SMS Filter mode

3. Select **Menu** → **Save** to save the changes.

CREATING THE BLACK LIST

The Black List contains entries of banned numbers, i.e., the numbers from which Call&SMS Filter blocks calls and SMS. Each entry contains the following information:

- Telephone number from which Call&SMS Filter blocks calls and / or SMS.
- Types of events that Call&SMS Filter blocks from this number. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase that Call&SMS Filter uses to classify an SMS as unsolicited (spam). Call&SMS Filter only blocks SMS containing the key phrase, while delivering all other SMS.

Call&SMS Filter blocks calls and SMS that comply with all the criteria of an entry on the Black List. Calls and SMS that fail to comply with even one of the criteria of an entry on the Black List will be allowed by Call&SMS Filter.

You cannot add a phone number with identical filtering criteria to both the Black List and the White List.

Information about blocked SMS and calls is registered in the log (see the "Application logs" section on page [49](#)).

IN THIS SECTION

Adding entries to the Black List	32
Editing entries in the Black List	33
Deleting entries from the Black List	34

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 Call&SMS Filter numbers at the same time. If a number with such filtering criteria is already saved on either of the lists, Kaspersky Mobile Security 9 will notify you of this event, and a relevant message will appear on the screen.

➡ To add an entry to the Call&SMS Filter Black List:

1. Select **Black List** in the **Call&SMS Filter** tab.

This will open the **Black List** window.

2. Select **Menu** → **Add**.

This will open the **New entry** window.

3. Set values for the following settings (see Figure below).

- **Block incoming** – type of event from a telephone number which Call&SMS Filter blocks for Black List numbers:
 - **Calls and SMS:** block incoming calls and SMS messages.
 - **Calls only:** block incoming calls only.
 - **SMS only:** block incoming SMS messages only.
- **Phone number** – telephone number for which Call&SMS Filter 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 amount of symbols, and "?" any one symbol). For example, *1234? on the Black List. Call&SMS Filter blocks calls or SMS from a number in which any symbol follows the figure 1234.
- **Containing text** – key phrase indicating that the received SMS message is unwanted (spam). Call&SMS Filter only blocks SMS containing the key phrase, while delivering all other SMS.

If you want all incoming SMS from a specific number on the Black List to be blocked, leave this entry's **Containing text** field blank.

Figure 4. Settings for entries in the Black List

4. Select **Menu** → **Save** to save the changes.

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 Call&SMS Filter Black List:

1. Select **Black List** in the **Call&SMS Filter** tab.

This will open the **Black List** window.

2. Select the element from the list which you wish to edit and then select **Menu** → **Edit**.

The **Changing an entry** screen opens.

3. Change the necessary settings:

- **Block incoming** – type of event from a telephone number which Call&SMS Filter blocks for Black List numbers:
 - **Calls and SMS**: block incoming calls and SMS messages.
 - **Calls only**: block incoming calls only.
 - **SMS only**: block incoming SMS messages only.
- **Phone number** – telephone number for which Call&SMS Filter 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 amount of symbols, and "?" any one symbol). For example, *1234? on the Black List. Call&SMS Filter blocks calls or SMS from a number in which any symbol follows the figure 1234.
- **Containing text** – key phrase indicating that the received SMS message is unwanted (spam). Call&SMS Filter only blocks SMS containing the key phrase, while delivering all other SMS.

If you want all incoming SMS from a specific number on the Black List to be blocked, leave this entry's **Containing text** field blank.

4. Select **Menu** → **Save** to save the changes.

DELETING ENTRIES FROM THE BLACK LIST

You can delete a number from the Black list. Furthermore, you can clear the Call&SMS Filter Black List by removing all the entries from it.

➡ *To delete an entry from the Call&SMS Filter Black List:*

1. Select **Black List** in the **Call&SMS Filter** tab.

This will open the **Black List** window.

2. Select the entry to be deleted on the list and then select **Menu** → **Delete**.

The confirmation window opens.

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

➡ *To clear the Call&SMS Filter Black List:*

1. Select **Black List** in the **Call&SMS Filter** tab.

This will open the **Black List** window.

2. Select **Menu** → **Delete all**.

The confirmation window opens.

3. 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 Call&SMS Filter delivers calls and SMS to the user. Each entry contains the following information:

- Telephone number from which Call&SMS Filter delivers calls and / or SMS.
- Types of events that Call&SMS Filter delivers from this number. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase used by Call&SMS Filter to classify an SMS as solicited (not spam). Call&SMS Filter only delivers SMS containing the key phrase, while blocking all other SMS.

Call&SMS Filter allows only calls and SMS that comply with all the criteria of an entry on the White List. Calls and SMS that fail to comply with even one of the criteria of an entry on the White List will be blocked by Call&SMS Filter.

IN THIS SECTION

Adding entries to the White List.....	35
Editing entries in the White List	36
Deleting entries from the White List	36

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 Call&SMS Filter numbers at the same time. If a number with such filtering criteria is already saved on either of the lists, Kaspersky Mobile Security 9 will notify you of this event, and a relevant message will appear on the screen.

➡ To add an entry to the Call&SMS Filter White List:

1. On the **Call&SMS Filter** tab, select the **White List**.

This will open the **White List** window.

2. Select the **Menu** → **Add**.

3. Make the following settings for the new entry (see Figure below).

- **Allow incoming** – type of event from a telephone number which Call&SMS Filter allows for Black List numbers:
 - **Calls and SMS:** allow incoming calls and SMS messages.
 - **Calls only:** allow incoming calls only.
 - **SMS only:** allow incoming SMS messages only.
- **Phone number** – telephone number for which Call&SMS Filter 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 amount of symbols, and "?" any one symbol). For example, *1234? in the White List. Call&SMS Filter delivers calls or SMS from a number in which any symbol follows the figure 1234.
- **Containing text** – key phrase indicating that the received SMS message is wanted. For numbers on the White List, Call&SMS Filter only delivers SMS messages containing the key phrase and blocks all others.

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

New entry

Allow incoming:

☐ Calls and SMS

☐ Calls only

☒ SMS only

Phone number:

987654321

Containing text:

payment

Figure 5. Settings for entries in the White List

4. Select **Menu** → **Save** to save the changes.

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 Call&SMS Filter White List:*

1. On the **Call&SMS Filter** tab, select the **White List**.

This will open the **White List** window.

2. Select the element from the list which you wish to edit and then select **Menu** → **Edit**.

The **Changing an entry** screen opens.

3. Change the necessary settings:

- **Allow incoming** – type of event from a telephone number which Call&SMS Filter allows for Black List numbers:
 - **Calls and SMS:** allow incoming calls and SMS messages.
 - **Calls only:** allow incoming calls only.
 - **SMS only:** allow incoming SMS messages only.
- **Phone number** – telephone number for which Call&SMS Filter 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 amount of symbols, and "?" any one symbol). For example, *1234? in the White List. Call&SMS Filter delivers calls or SMS from a number in which any symbol follows the figure 1234.
- **Containing text** – key phrase indicating that the received SMS message is wanted. For numbers on the White List, Call&SMS Filter only delivers SMS messages containing the key phrase and blocks all others.

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

4. Select **Menu** → **Save** to save the changes.

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 Call&SMS Filter White List:*

1. On the **Call&SMS Filter** tab, select the **White List**.

This will open the **White List** window.

2. Select the entry to be deleted on the list and then select **Menu** → **Delete**.

The confirmation window opens.

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

➡ *To clear the Call&SMS Filter White List:*

1. On the **Call&SMS Filter** tab, select the **White List**.

This will open the **White List** window.

2. Press **Menu** → **Delete all**.

The confirmation window opens.

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

The White List is emptied.

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

If the **Both lists** or **White List** modes (see the "**About Call&SMS Filter modes**" section on page [30](#)) are selected for Call&SMS Filter, you can additionally set a response from Call&SMS Filter to SMS and calls from subscribers, whose numbers are not saved in Contacts. In addition, Call&SMS Filter allows expansion of the White List by adding numbers from the list of contacts to it.

➡ To select Call&SMS Filter's response to a number not included in the phonebook:

1. Select the **Mode** menu item on the **Call&SMS Filter** tab.

The **Call&SMS Filter** opens.

2. Select the required value for setting **Allow Contacts** (see Figure below).
 - for Call&SMS Filter to count numbers from Contacts as additional White List and block SMS messages and calls from subscribers not in Contacts, check the **Allow Contacts** box;
 - in order for Call&SMS Filter to filter SMS messages and calls based on the Call&SMS Filter mode set, uncheck the **Allow contacts** box.

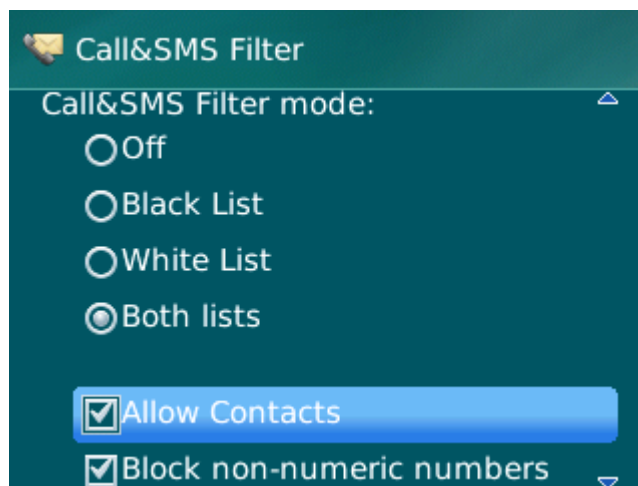


Figure 6. Call&SMS Filter response to numbers not included in the device's phone book

3. Select **Menu** → **Save** to save the changes.

RESPONDING TO SMS MESSAGES FROM NON-NUMERIC NUMBERS

If the Call&SMS Filter mode **Both lists** or **Black List** is selected (see the "**About Call&SMS Filter modes**" section on page 30), you can also expand the Black List by including all non-numeric numbers (including letters). In this case, Call&SMS Filter processes calls and SMS messages from non-numeric numbers the same way as from numbers on the Black List.

➡ To set Call&SMS Filter's response when receiving messages from non-numeric numbers:

1. On the **Call&SMS Filter** tab, select the menu item **Mode**.
2. The **Call&SMS Filter** opens.
3. Select a value for the **Block non-numeric numbers** setting (see Figure below).
 - in order for Call&SMS Filter to block SMS from non-numeric numbers, check the **Block non-numeric numbers** box;
 - In order for Call&SMS Filter to filter SMS from non-numeric numbers on the basis of the Anti-Spam mode set, uncheck the **Block non-numeric numbers** box.

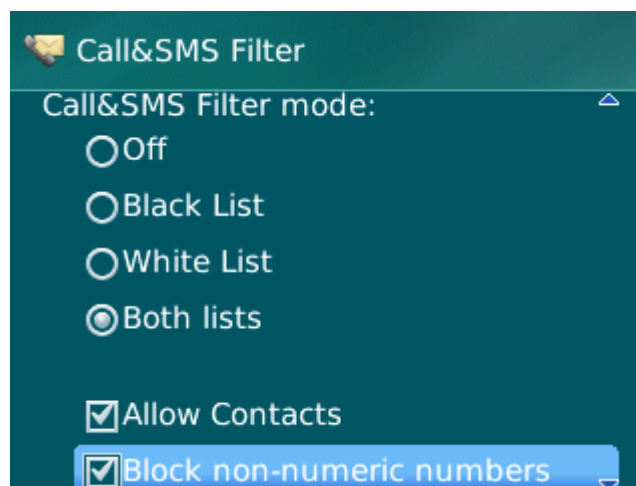


Figure 7. Configuring Call&SMS Filter action when receiving SMS messages from non-numeric numbers

4. Select **Menu** → **Save** to save the changes.

SELECTING A RESPONSE TO INCOMING SMS

In **Both lists** mode (see the "**About Call&SMS Filter modes**" section on page 30), Call&SMS Filter checks incoming SMS against the Black and White lists.

After receiving an SMS message from a number that is not included on either list, Call&SMS Filter will prompt you to enter the number in one of the lists (see Figure below).

You can select one of the following actions to be performed in respect of the SMS:

- To block the SMS message and add the sender's telephone number to the Black List, select **Add to Black List**.
- To deliver the SMS message and add the sender's telephone number to the White List, select **Add to White List**.

- To deliver the SMS message without adding the sender's telephone number to either list, press **Skip**.



Figure 8. Call&SMS Filter notification about the receipt of an SMS

Information about blocked SMS is registered in the application's log (see the "Application logs" section on page [49](#)).

SELECTING RESPONSE TO INCOMING CALLS

In **Both lists** mode (see the "About Call&SMS Filter modes" section on page [30](#)), Call&SMS Filter checks incoming calls according to the Black and White lists. Following a call received from a number on neither list, Call&SMS Filter will prompt you to enter the number in one of the lists (see Figure below).

You can select one of the following actions for the number from which the call was made:

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



Figure 9. Call&SMS Filter notification about the receipt of an SMS

Information about blocked calls is registered in the application's log (see the "Application logs" section on page [49](#)).

DATA PROTECTION IN THE EVENT OF LOSS OR THEFT OF THE DEVICE

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 the parameters of its operation and start Anti-Theft from another mobile device remotely.

IN THIS SECTION

About Anti-Theft	40
Blocking the device	41
Deleting personal data	42
Creating a list of folders to delete	44
Monitoring the replacement of a SIM card on the device	45
Determining the device's geographical coordinates	46
Starting Anti-Theft functions remotely	47

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.
- **Data Wipe** – can remotely delete the user's personal data from the device (entries in Contacts, SMS, picture gallery, calendar, logs, Internet connection settings) and information from the storage cards, folders from list for deletion.
- **SIM Watch** allows obtaining the current phone number in the event that the SIM card is replaced, as well as locking the device in the event the SIM card is replaced or the device is activated without a SIM card. Information about a new telephone number is sent as a message to a 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.

After installing Kaspersky Mobile Security 9, all Anti-Theft functions are disabled.

Kaspersky Mobile Security 9 can remotely start Anti-Theft with sending SMS commands from another mobile device.

To start Anti-Theft remotely, you have to know the secret code set when Kaspersky Mobile Security 9 was first started.

The current status of every function is displayed in the **Anti-Theft** screen next to the name of the function.

Information about the component's operation is entered in the application's log (see "Application Logs" on page [49](#)).

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.

➡ To enable the Block function:

1. Select the **Block** item on the **Anti-Theft** tab.

This will open the **Block** window.

2. Check the **Enable Block** box.
3. Enter the message which is displayed on the device's 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 telephone is used for the message.

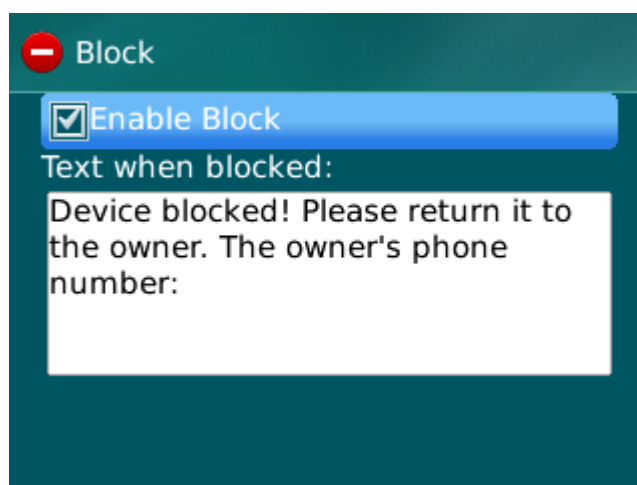


Figure 10. Block function settings

4. Select **Menu** → **Save** to save the changes.

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 Mobile Security 9, 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. As a result, your device will receive a covert SMS, and the device will be blocked.

Outgoing SMS messages will be billed at the rates set by the other mobile device's mobile service provider.

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. Select the **Send command** menu item on the **Additional** tab.
This will open the **Send command** window.
2. For the **Select SMS command** setting, select **Block**.
3. In the **Phone number** field, enter the phone number of the device that receives the SMS command.
4. In the **Remote device code** field, enter the application secret code set on the device that receives the SMS command.
5. Select **Menu** → **Send**.

➡ To create an SMS with the phone's standard SMS creation functions,

send a standard SMS to another device; it should contain the text `block:<code>`, where `<code>` is the secret code of the application set on another device. 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, calendar, email messages, call log);
- information on storage card;
- files from the list of objects for deletion (see the "Creating a list of folders to delete" section on page [44](#)).

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. Select the **Data Wipe** item on the **Anti-Theft** tab.
This will open the **Data Wipe** screen.
2. Select the **Mode** item.
This will open the **Data Wipe** screen.
3. Check the **Enable Data Wipe** box.
4. Select information that you want to delete. To do this, check the boxes next to the required settings in the **Delete** section (see Figure below).
 - to delete personal data, check the **Personal data** box;
 - to delete files from folders on the memory card and from the list of objects for deletion, check the box **Selected folders**.

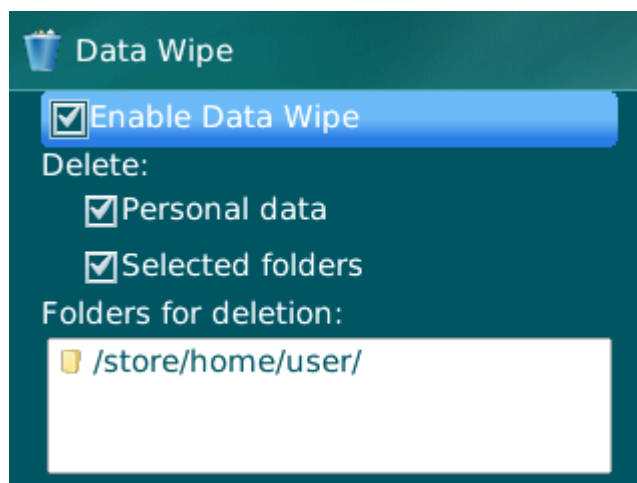


Figure 11. Data Wipe function settings

5. Go to creation of a list of objects for deletion (see the "Creating a list of folders to delete" section on page [44](#)).
6. Select **Menu** → **Save** to save the changes.

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 Mobile Security 9, on another mobile device to create and send an SMS command to your device. As a result, your device receives a covert SMS message after which the information is deleted. To create a special SMS command, use the Sending a 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 after which the information is deleted.

Outgoing SMS messages will be billed at the rates set by the other mobile device's mobile service provider.

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. Select the **Send command** menu item on the **Additional** tab.

This will open the **Send command** window.

2. For the **Select SMS command** setting, select **Data Wipe**.
3. In the **Phone number** field, enter the phone number of the device that receives the SMS command.
4. In the **Remote device code** field, enter the application secret code set on the device that receives the SMS command.
5. Select **Menu** → **Send**.

➡ To create an SMS with the phone's standard SMS creation functions:

send a standard SMS to another device; it should contain the text `wipe:<code>` where `<code>` is the secret code of the application set on another 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.

For Anti-Theft to delete the objects from the list after receiving a special SMS command, ensure that **Selected folders** is checked on the **Anti-Theft** → **Data Wipe** tab.

The administrator may add to the list of folders to be deleted. These folders cannot be deleted from the list.

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

1. Select the **Data Wipe** item on the **Anti-Theft** tab.

This will open the **Data Wipe** screen.

2. Go to the list of objects for deletion.
3. Select **Menu** → **Add folder** (see Figure below).

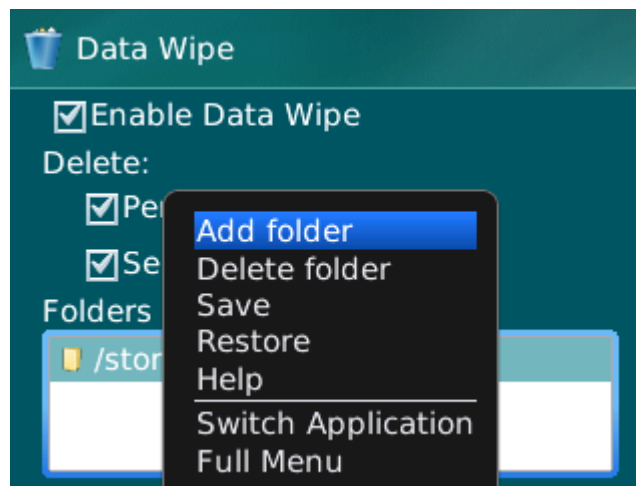


Figure 12. Adding folders

4. Select the necessary folder from the folder tree and press **Menu** → **Select**.

The folder is added to the **Selected folders** list.

5. Select **Menu** → **Save**.

➡ To remove a folder from the list:

1. Select the **Data Wipe** item on the **Anti-Theft** tab.

This will open the **Data Wipe** screen.

2. Go to the list of objects for deletion.
3. Select the folder from the list and then select **Menu** → **Delete folder**.

The confirmation window opens.

4. Confirm the deleting of the folder by pressing **Yes**.

The folder will be deleted from the **Selected folders** list.

5. Select **Menu** → **Save**.

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 **Anti-Theft** tab, select the **SIM Watch** item.

This will open the **SIM Watch** window.

2. Check the **Enable SIM Watch** box.

3. To check the replacement of the SIM card on the device, make the following settings (see Figure below).

- To automatically receive an SMS message with the new number being used in your telephone, enter the telephone number to which the SMS message should be sent in the **SMS to phone number** field within the **When the SIM card is replaced, send the new number** box.

The phone number may begin with a digit or with a "+", and must contain digits only.

- To receive an email with the new telephone number, in the **When the SIM card is replaced, send the new number** block in the **Message to email** field, 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 device** box in the **Additional** block. You can unblock the device only by entering the application secret code.
- To display a message on the screen in blocked mode, enter it in the **Text when blocked** field. By default, the standard text in which you can add the owner's number is used for the message.

Figure 13. SIM Watch function settings

4. Select **Menu** → **Save** to save the changes.

DETERMINING THE DEVICE'S GEOGRAPHICAL COORDINATES

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

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

This function only works with devices with in-built GPS receiver. The GPS receiver is enabled automatically after the device receives a special SMS command. If the device is within the area reached by satellites, the GPS Find function receives and sends the geographical coordinates of the device. If the satellites are unavailable at the time of the query, GPS Find will periodically re-attempt to find them and send device location results.

➡ To enable the GPS Find function:

1. Select the **GPS Find** item on the **Anti-Theft** tab.

This will open the **GPS Find** window.

2. Check the **Enable GPS Find** box.

After receiving a special SMS command, Kaspersky Mobile Security 9 sends the device's coordinates by return SMS.

3. To receive the coordinates of the device by email, in the **Send device coordinates** block for the setting **Message to email** enter email address (see Figure below).

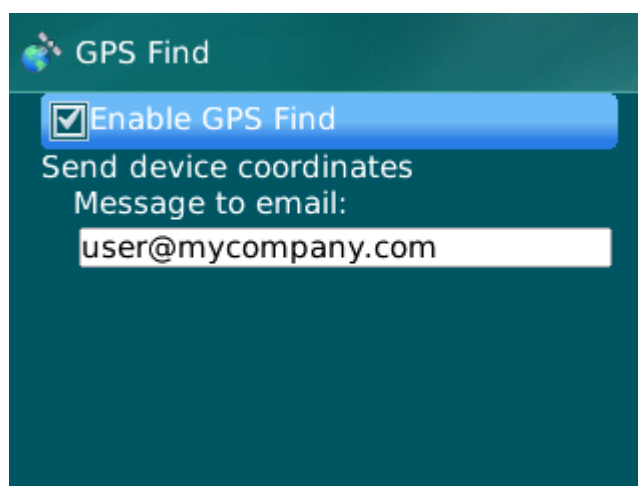


Figure 14. GPS Find function settings

4. Select **Menu** → **Save** to save the changes.

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 Mobile Security 9, 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's coordinates. To create a special SMS command, use the Sending a 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 a covert SMS, and the application will send the device's coordinates.

Outgoing SMS messages will be billed at the rates set by the other mobile device's mobile service provider.

To receive the device's location, 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. Select the **Send command** menu item on the **Additional** tab.

This will open the **Send command** window.

2. Select the **GPS Find** value for the **Select SMS command** setting.
3. In the **Phone number** field, enter the phone number of the device that receives the SMS command.
4. In the **Remote device code** field, enter the application secret code set on the device that receives the SMS command.
5. Select **Menu** → **Send**.

➡ To create an SMS with the phone's standard SMS creation functions:

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

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

STARTING ANTI-THEFT FUNCTIONS REMOTELY

The application allows sending a special SMS command to run Anti-Theft functions remotely on another device with Kaspersky Mobile Security 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 at your mobile service provider's current rate.

➡ To send an SMS command to another device:

1. Select the **Send command** item on the **Additional** tab.

This will open the **Send command** window.

2. Select the function for remote launch on another mobile device. Select one of the proposed values for the **Select SMS command** setting (see Figure below).
 - Block device (on page [41](#)).
 - Data Wipe (see "Deleting personal data" section on page [42](#)).
 - GPS Find (see the "Determining the device's geographical coordinates" section on page [46](#)).

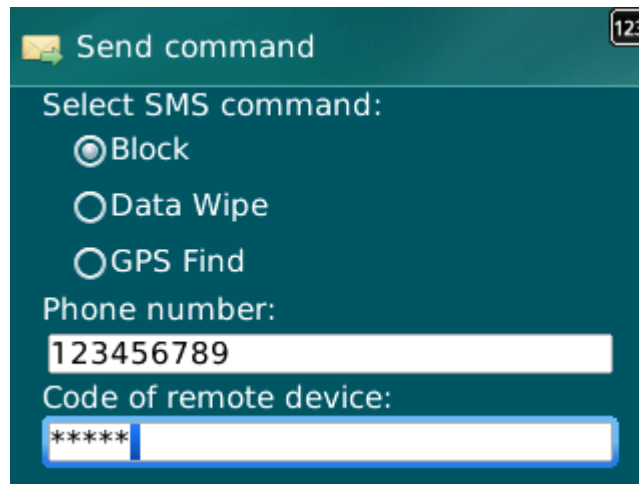


Figure 15. Remote startup of Anti-Theft and Privacy Protection functions

3. In the **Phone number** field, enter the phone number of the device that receives the SMS command.
4. In the **Remote device code** field, enter the application secret code set on the device that receives the SMS command.
5. Select **Menu** → **Send**.

APPLICATION LOGS

This section gives information about logs, in which each component's operations are recorded, as well as each task that is completed (e.g. receipt of an SMS command from another device).

IN THIS SECTION

About logs	49
Viewing Log records.....	49
Deleting log records	49

ABOUT LOGS

The application's logs store records about events that occur during Kaspersky Mobile Security 9 operation. Entries are sorted by time of the event and starting with the most recent events.

For every component, a separate events log is used.

VIEWING LOG RECORDS

- *To view the entries in a component's log,*
on the tab of the necessary component, select the item **Events log**.

The selected component's log opens.

Use the scroll bar to scroll through the log.

- *To view detailed log record information,*
select the necessary entry and press **ENTER** on the keyboard.

DELETING LOG RECORDS

You can clear all logs. Information on the operation of all components of Kaspersky Mobile Security 9 will be deleted.

- *To clear all logs:*
 1. On the tab of any component, select the **Events log**.
The **Events log** window opens.
 2. Select **Menu** → **Clear Log**.
 3. Confirm the uninstalling by pressing the **Yes** button.

All entries from all components' logs will be deleted.

CONFIGURING ADDITIONAL SETTINGS

This section provides information on additional options of Kaspersky Mobile Security 9: how to change the secret code and how to enable/disable the display of the hints.

IN THIS SECTION

Changing the secret code	50
Displaying prompts.....	50

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. Select the **Additional settings** menu item on the **Additional** tab.
The **Additional settings** screen opens.
2. Select **Change code**.
3. Enter the current secret code of the application in the **Enter code** entry field.
4. Enter the new secret code in the **Enter new code** and **Confirm code** fields.

The code entered is automatically verified.

If the secret code entered is valid, it will be saved.

If the code is deemed invalid according to the results of the verification, a warning message is displayed and the application requests confirmation. To use the code, press **Yes**.

In order to create a new code, press **No**. The **Enter new code** and **Confirm code** fields will empty. Enter a new application secret code.

DISPLAYING PROMPTS

When you configure the settings of components, Kaspersky Mobile Security 9 displays by default a prompt with a short description of the function selected. You can configure the display of Kaspersky Mobile Security 9 hints.

➡ *To configure the display of hints, perform the following steps:*

1. Select the **Additional settings** menu item on the **Additional** tab.
The **Additional settings** screen opens.
2. Enable / disable the display of prompts. To do this, select **Hints**.

The status of the display of prompts will be shown next to the **Hints** menu item. The radio button icon to the right changes according to the status of the display of prompts.

CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and what conditions should be met to receive help from the Technical Support Service.

IN THIS SECTION

How to get technical support	51
Technical support by phone	51
Obtaining technical support via My Kaspersky Account	52

HOW TO GET TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (see section "Sources of information about the application" on page [Error! Bookmark not defined.](#)), we recommend that you contact Kaspersky Lab's Technical Support Service. Technical Support Service specialists will answer any of your questions about installing and using the application. If your mobile device is infected, our specialists will help you fix any problems caused by malware.

Before contacting the Technical Support Service, please read the support rules (<http://support.kaspersky.com/support/rules>).

You can contact the Technical Support Service in one of the following ways:

- By phone. This method allows you to consult with specialists from our Russian-language or international Technical Support Service.
- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact our specialists using the query form.

To qualify for technical support, you must be a registered user of a commercial version of Kaspersky Mobile Security. Technical support is not available to users of trial versions of the application.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from the Russian-speaking or international Technical Support Service by phone (<http://support.kaspersky.com/support/international>).

Before contacting the Technical Support Service, you should collect information (<http://support.kaspersky.com/support/details>) about your mobile device and anti-virus applications installed on it. This will enable our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

My Kaspersky Account is your personal area (<https://my.kaspersky.com>) on the Technical Support Service website.

To obtain access to My Kaspersky Account, you should go through the registration procedure on the registration page (<https://my.kaspersky.com/registration>). Enter your email address and a password to log in to My Kaspersky Account.

In My Kaspersky Account, you can perform the following actions:

- contact the Technical Support Service and Virus Lab;
- contact the Technical Support Service without using email;
- track the status of your request in real time;
- view a detailed history of your requests to the Technical Support Service;
- receive a copy of the key file if it has been lost or removed.

E-mailing your question to the Technical Support Service

You can send an online request to the Technical Support Service in Russian, English, German, French, or Spanish.

You should specify the following data in the fields of the online request form:

- request type;
- application name and version number;
- request description;
- customer ID and password;
- email address.

A specialist from the Technical Support Service sends an answer to your question to your My Kaspersky Account and to the email address that you have specified in your online request.

Online request to the Virus Lab

Some requests should be sent to the Virus Lab instead of the Technical Support Service.

You can send requests of the following types to the Virus Lab:

- *Unknown malicious program* – you suspect that a file contains a virus but Kaspersky Mobile Security has not identified it as infected.

Virus Lab specialists analyze malicious code sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- *False alarm* – Kaspersky Mobile Security classifies the file as a virus, yet you are sure that the file is not a virus.
- *Request for description of malicious program* – you want to receive the description of a virus detected by Kaspersky Mobile Security, using the name of the virus.

You can also send requests to the Virus Lab from the page with the request form (<http://support.kaspersky.com/virlab/helpdesk.html>) without being registered in My Kaspersky Account. On this page, you do not have to specify the application activation code.

GLOSSARY

A

ACTIVATING THE APPLICATION

Switching the application into full-function mode. The user needs a license to activate the application.

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.

B

BLACK LIST

The entries in this list contain the following information:

- *Telephone number* from which Call&SMS Filter blocks calls and / or SMS.
- *Types of events* that Call&SMS Filter blocks from this number. The following types of events are available: calls and SMS, calls only, and SMS only.
- *Key phrase* that Call&SMS Filter uses to classify an SMS as unsolicited (spam). Call&SMS Filter only blocks SMS containing the key phrase, while delivering all other SMS.

D

DELETING SMS MESSAGES

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.

N

NON-NUMERIC NUMBER

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

T

TELEPHONE NUMBER MASK

Putting a telephone number in the Black or White List using wildcards. The two basic wildcards used in telephone number masks are "*" and "?", (where "*" represents any number of characters and "?" stands for any single character). For example, *1234? on the Black List. Call&SMS Filter blocks calls or SMS from a number in which any symbol follows the figure 1234.

W**WHITE LIST**

The entries in this list contain the following information:

- *Telephone number* from which Call&SMS Filter delivers calls and / or SMS.
- *Types of events* that Call&SMS Filter delivers from this number. The following types of events are available: calls and SMS, calls only, and SMS only.
- *Key phrase* used by Call&SMS Filter to classify an SMS as solicited (not spam). Call&SMS Filter only delivers SMS containing the key phrase, while blocking all other SMS.

KASPERSKY LAB

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

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

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

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, and gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company's specialists to foresee trends in the development of malware and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Many well-known manufacturers use the Kaspersky Anti-Virus @kernel in their products, including: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

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

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. Detailed consultations are provided by phone or email. You will receive full answers to all of your questions.

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

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

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

Kaspersky Lab 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	57
Other information	59

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.....	57
ADBWINAPI.DLL	57
ADBWINUSBAPI.DLL	57

ADB

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

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

Additional information about third-party code.

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

CryptoEx LLC corporate website: <http://www.cryptoex.ru>

INDEX

A

Activating the application.....	20
license	27
Adding	
Call&SMS Filter Black List.....	36
Call&SMS Filter White List.....	39
Allowing	
incoming calls	39
incoming SMS	39
Anti-Theft.....	44
Block.....	45
Data Wipe.....	46, 48
GPS Find.....	50
SIM Watch	49
Application secret code	23, 24, 54

B

Black List	
Call&SMS Filter	35
Blocking	
device	45
incoming calls	35, 38
incoming SMS	35

C

Call&SMS Filter.....	34
action on call.....	43
action on SMS	42
Black List.....	35
modes.....	34
non-numeric numbers.....	42
numbers out of Contacts.....	41
White list.....	38
Code	
activation code.....	21, 22
application secret code	23

D

Data	
remote delete.....	46
Delete	
Call&SMS Filter Black List.....	38
Call&SMS Filter White List.....	40
Deleting	
Log records.....	53
Determining the device's location.....	50
Disabling	
Call&SMS Filter	34, 35

E

Edit	
Call&SMS Filter Black List.....	37
Call&SMS Filter White List.....	40
Enabling	

Call&SMS Filter	35
Entry	
Call&SMS Filter Black List.....	36
Call&SMS Filter White List.....	39
Events log	
deleting entries	53
viewing entries	53
F	
FILTERING	
INCOMING CALLS.....	34
INCOMING SMS	34
H	
Hardware requirements.....	17
I	
INSTALLING THE APPLICATION	18
L	
License	
activating the application	20
information.....	28
License Agreement.....	27
renewal	29
M	
Modes	
Call&SMS Filter	34, 35
R	
Renewing the license	29
S	
Send SMS command	51
Starting	
application	25
U	
UNINSTALLING	
APPLICATION.....	19
W	
White list	
Call&SMS Filter	38
Wipe	
information saved on the device	46