

Kaspersky Mobile Security 9

*for Android OS*

**KASPERSKY** **lab**

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: 20.01.2011

© 1997-2011 Kaspersky Lab ZAO. All Rights Reserved.

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

## KASPERSKY LAB END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

### 1. Definitions

- 1.1. **Software** means software including any Updates and related materials.
- 1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.
- 1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.
- 1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.
- 1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.
- 1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.
- 1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

### 2. Grant of License

- 2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:  
Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.  
Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.
- 2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package or as specified in additional agreement.
- 2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You acquired the License to the Software or as specified in additional agreement.
- 2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is

terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.

- 2.5. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):
- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
  - Technical Support via the Internet and Technical Support telephone hotline.

### **3. Activation and Term**

- 3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.
- 3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement or as specified in additional agreement.
- 3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition or as specified in additional agreement.
- 3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (7 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline. If Rightholder sets another duration for the single applicable evaluation period You will be informed via notification.
- 3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.
- 3.6. If You have acquired the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
- 3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.
- 3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.
- 3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.
- 3.10. If You have acquired the Software with activation code valid for language localization of the Software of that region in which it was acquired from the Rightholder or its Partners, You cannot activate the Software with applying the activation code intended for other language localization.
- 3.11. If You have acquired the Software intended for operation with particular telecoms operator such the Software may be used only for operation with operator specified during acquisition.
- 3.12. In case of limitations specified in Clauses 3.10 and 3.11 information about these limitations is stated on package and/or website of the Rightholder and/or its Partners.

### **4. Technical Support**

The Technical Support described in Clause 2.5 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: <http://support.kaspersky.com>

### **5. Limitations**

- 5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

- 5.2. You shall not transfer the rights to use the Software to any third party except as set forth in additional agreement.
- 5.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in additional agreement.
- 5.4. You shall not rent, lease or lend the Software to any third party.
- 5.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.
- 5.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.
- 5.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

## **6. Limited Warranty and Disclaimer**

- 6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.
- 6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.
- 6.3. You acknowledge, accept and agree that Rightholder is not responsible or liable for data deletion authorized by You. The mentioned data may include any personal or confidential information.
- 6.4. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.
- 6.5. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.5 of this Agreement.
- 6.6. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.
- 6.7. THE SOFTWARE IS PROVIDED "AS IS" AND THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE Rightholder AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE Rightholder .

## **7. Exclusion and Limitation of Liability**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE Rightholder OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY

BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE Rightholder OR ANY OF ITS PARTNERS, EVEN IF THE Rightholder OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE Rightholder AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE Rightholder AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE Rightholder OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

## **8. GNU and Other Third Party Licenses**

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to [source@kaspersky.com](mailto:source@kaspersky.com) or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

## **9. Intellectual Property Ownership**

- 9.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.
- 9.2 You acknowledge that the source code, activation code and/or license key file for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.
- 9.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

## **10. Governing Law; Arbitration**

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

**11. Period for Bringing Actions**

No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

**12. Entire Agreement; Severability; No Waiver**

This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

**13. Rightholder Contact Information**

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1<sup>st</sup> Volokolamsky Proezd  
Moscow, 123060  
Russian Federation  
Tel: +7-495-797-8700  
Fax: +7-495-645-7939  
E-mail: [info@kaspersky.com](mailto:info@kaspersky.com)  
Web site: [www.kaspersky.com](http://www.kaspersky.com)

© 1997-2011 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

# TABLE OF CONTENTS

ABOUT THIS GUIDE .....	11
In this document .....	11
Document conventions .....	13
ADDITIONAL DATA SOURCES .....	15
Information sources for further research.....	15
Contacting the Sales Department.....	16
Discussion of Kaspersky Lab applications on the Web forum .....	16
Contacting the Documentation Development Group .....	16
KASPERSKY MOBILE SECURITY 9.....	17
Hardware and software requirements.....	18
Distribution kit.....	18
INSTALLING KASPERSKY MOBILE SECURITY 9 .....	19
UNINSTALLING THE APPLICATION .....	20
GETTING STARTED.....	21
Activating the application.....	21
Activating the commercial version.....	22
Activating the subscription for Kaspersky Mobile Security 9 .....	23
Purchasing an activation code online.....	23
Activating the trial version .....	24
Setting the secret code.....	24
Enabling the option to recover the secret code.....	25
Recovering the secret code .....	25
Starting the application .....	26
Viewing information about the application .....	26
MANAGING THE LICENSE .....	27
About the License Agreement .....	27
About Kaspersky Mobile Security 9 licenses .....	27
View License Information.....	28
Renewing the license .....	29
Renewing the license with the activation code.....	29
Renewing the license online .....	30
Renewing the license by activating a subscription .....	30
Unsubscribing .....	31
Renewing the subscription.....	31
APPLICATION INTERFACE .....	32
Protection status window.....	32
Home screen widget.....	33
FILE SYSTEM PROTECTION .....	34
About Protection .....	34
Activate/Deactivate Protection.....	34
Configuring the protection area .....	36
Selecting the action to be performed on detected objects .....	37

SCANNING THE DEVICE .....	38
About scanning the device.....	38
Starting a scan manually .....	38
Starting a scheduled scan .....	40
Selection of object type to be scanned .....	41
Configuring archive scans .....	42
Selecting the action to be performed on detected objects .....	42
FILTERING OF INCOMING CALLS AND SMS.....	44
About Call&SMS Filter.....	44
About Call&SMS Filter modes .....	45
Changing the Call&SMS Filter mode .....	45
Creating the Black List.....	46
Adding entries to the Black List.....	47
Editing entries in the Black List .....	48
Deleting entries from the Black List.....	49
Creating a White List .....	49
Adding entries to the White List .....	50
Editing entries in the White List.....	51
Deleting entries from the White List .....	52
Responding to SMS messages and calls from contacts not in the phone book.....	52
Responding to SMS messages from non-numeric numbers.....	53
Selecting a response to incoming SMS .....	54
Selecting response to incoming calls.....	55
Viewing Log records .....	56
DATA PROTECTION IN THE EVENT OF LOSS OR THEFT OF THE DEVICE .....	58
About Anti-Theft.....	58
Blocking the device.....	59
Deleting personal data.....	60
Creating a list of folders to delete .....	62
Monitoring the replacement of a SIM card on the device.....	63
Determining the device's geographical coordinates.....	65
Starting Anti-Theft functions remotely.....	67
PRIVACY PROTECTION .....	69
Privacy Protection.....	69
Privacy Protection modes .....	69
Enabling/disabling Privacy Protection.....	70
Enabling Privacy Protection automatically .....	70
Enabling Privacy Protection remotely .....	72
Selecting data to hide: Privacy Protection .....	73
Creating a list of private numbers .....	74
Adding a number to the list of private numbers.....	75
Editing a number in the list of private numbers .....	76
Deleting a number from the list of private numbers.....	77
UPDATING THE APPLICATION'S DATABASES .....	78
About updating the application's databases .....	78
Starting updates manually .....	79
Starting scheduled updates .....	79

CONFIGURING ADDITIONAL SETTINGS .....80

- Changing the secret code.....80
- Displaying prompts .....80
- Configuring sound notifications.....81
- Messages in the status line .....81

CONTACTING THE TECHNICAL SUPPORT SERVICE .....83

GLOSSARY .....84

KASPERSKY LAB.....86

INFORMATION ABOUT THIRD PARTY CODE.....87

- Distributed program code .....87
  - ADB .....87
  - ADBWINAPI.DLL .....87
  - ADBWINUSBAPI.DLL.....87
- Other information.....89

INDEX .....90

# ABOUT THIS GUIDE

This document is the Guide for the installation, configuration and use of Kaspersky Mobile Security 9. The document is designed for a wide audience.

Objectives of the document:

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

## IN THIS SECTION

---

In this document.....	<a href="#">11</a>
Document conventions.....	<a href="#">13</a>

## IN THIS DOCUMENT

The following sections are included in the document:

### Additional data sources

This section contains a description of additional sources of information about the application and on Internet resources where you can discuss the program, share ideas, ask questions and receive answers to them.

### Kaspersky Mobile Security 9

This section contains a description of the application's options as well as brief information about its individual components and main functions. From this section, you can learn about the function of the installation package. The section contains the device and program requirements which the mobile device must meet in order to install Kaspersky Mobile Security 9.

### Installing Kaspersky Mobile Security 9

This section contains instructions which will help you to install the application on a mobile device.

### Uninstalling the application

This section contains instructions which will help you to uninstall the application from a mobile device.

### Updating the application

This section contains instructions which will help you to update the application's previous version.

## Getting started

This section contains information about how to start working with Kaspersky Mobile Security 9: activate it, set the application's secret code, enable the function of recovering the secret code, recover the secret code, start the application, update its anti-virus databases and scan the device for viruses.

## Managing the license

This section contains information on the main terms used within the context of licensing the application. 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 on contacting Kaspersky Lab for help from the personal office on the technical support website and by telephone.

## **Glossary**

This section contains a list of terms which are found in the document and their definition.

## **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**

Document conventions described in the table below are used in this Guide.

Table 1. Document conventions

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

# ADDITIONAL DATA SOURCES

If you have questions about setting up or using Kaspersky Mobile Security 9, you can find answers from them, using various sources of information. You can choose the most suitable source according to how important or urgent your request is.

## IN THIS SECTION

---

Information sources for further research .....	<a href="#">15</a>
Contacting the Sales Department .....	<a href="#">16</a>
Discussion of Kaspersky Lab applications on the Web forum .....	<a href="#">16</a>
Contacting the Documentation Development Group .....	<a href="#">16</a>

## INFORMATION SOURCES FOR FURTHER RESEARCH

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

- the Kaspersky Lab application website;
- the application's Knowledge Base page at the Technical Support Service website;
- the installed Help system and hints;
- the installed application documentation.

### Page on Kaspersky Lab website

[http://www.kaspersky.com/kaspersky\\_mobile\\_security](http://www.kaspersky.com/kaspersky_mobile_security)

This page will provide you with general information about Kaspersky Mobile Security 9 and its features and options. You can also purchase Kaspersky Mobile Security 9 at our E-Store.

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

<http://support.kaspersky.com>

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

These articles contain useful information, recommendations and Frequently Asked Questions (FAQs) relating to the purchase, installation and use of Kaspersky Mobile Security 9. They are arranged in topics, such as "Database updates" and "Troubleshooting". The articles may answer questions about not only Kaspersky Mobile Security 9, but other Kaspersky Lab products too. They may also contain news from the Technical Support Service.

### The installed Help system

If you have any questions about specific windows or tabs in Kaspersky Mobile Security 9, you can view the context help.

In order to open context help, open the window you are interested in and select the item **Help**.

## The installed Documentation

The User Guide contains detailed information about the application's functions and how to use Kaspersky Mobile Security 9, together with advice and recommendations about configuring the application.

The documents are included in PDF format in the Kaspersky Mobile Security 9 distribution package.

You can also download these documents in electronic format from Kaspersky Lab's website.

## CONTACTING THE SALES DEPARTMENT

If you have questions about selecting or purchasing Kaspersky Mobile Security, or extending your license, please phone the Sales Department specialists in our Central Office in Moscow, at:

**+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00**

The service is provided in Russian or English.

You can also send your questions to the Sales Department by email, at [sales@kaspersky.com](mailto:sales@kaspersky.com).

## DISCUSSION OF KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users of Kaspersky Lab's anti-virus applications in our forum at <http://forum.kaspersky.com>.

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

## CONTACTING THE DOCUMENTATION DEVELOPMENT GROUP

If you have any questions about the documentation, or you have found an error in it, or would like to leave a comment, please contact our User documentation development group. To contact the Documentation Development Group send an email to [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com). Use the subject line: "Kaspersky Help Feedback: Kaspersky Mobile Security 9".

# KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 protects mobile devices (hereafter "devices") running Android OS operating system. The application can protect information on the device from infection by known threats, prevent unwanted SMS messages and calls, protect information on the device in case of theft or loss, and hide information relating to confidential contacts. Every type of threat is processed in separate components of the program. This allows to fine-tune the application settings depending on user needs.

Kaspersky Mobile Security 9 includes the following protection components:

- **Anti-Virus.** It protects the file system of the mobile device from viruses and other malicious applications. Anti-Virus can detect and neutralize malicious objects on your device and update the application's anti-virus databases.
- **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 folder.** This protects information on the device from unauthorized access when it is lost or stolen and also makes it easier to find. Anti-Theft enables you to lock your device remotely, delete any information stored there, and pinpoint its geographic location using SMS commands from another device. Furthermore, Anti-Theft allows you to lock your device if the SIM card is replaced or if the device is activated without a SIM card.
- **Privacy Protection.** It hides information related to confidential numbers from the contact list. For these numbers, Privacy Protection hides the entries in Contacts, the history of calls and SMS, incoming calls and SMS.

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

## IN THIS SECTION

---

Hardware and software requirements .....	<a href="#">18</a>
Distribution kit.....	<a href="#">18</a>

## **HARDWARE AND SOFTWARE REQUIREMENTS**

Kaspersky Mobile Security 9 can be installed on mobile devices working on Android OS 1.5, 1.6, 2.0, 2.1, 2.2.

## **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](mailto:sales@kaspersky.com).

# INSTALLING KASPERSKY MOBILE SECURITY 9

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

➤ *To install Kaspersky Mobile Security 9:*

1. Copy the application's distribution package to your device, To do this, perform one of the following actions:
  - When buying the application on CD, connect the mobile device to the computer and start the automatic Kaspersky Mobile Security 9 installation on the disc purchased.
  - When obtaining the application's distribution package via the Internet, connect the mobile device to the computer and copy the application's distribution package to it.
  - Copy the application's distribution package to the mobile device from the Kaspersky Lab online store (<http://www.kaspersky.com/globalstore>).

2. Run the application's installation. To do this, open the ARK archive of the distribution package on the mobile device.

The application's installation wizards starts. When the wizards finishes, the application is installed with the parameters recommended by Kaspersky Lab specialists.

3. Open the application. To do this, in the main window switch to the applications window, select **Kaspersky Mobile Security 9** and run the application.
4. Read the License Agreement text, which is concluded between you and Kaspersky Lab. If you agree to all terms of the agreement, press **Accept**. Then the **Activation** window will open. If you do not agree to the terms of the License Agreement, press **Decline**. The application ends.
5. Run the application (see "Activating the application" on page [21](#)).
6. Enter the new application secret code. To do this, successively fill in the fields **Set a new secret code** and **Re-enter a new code** and click the **Enter** key.

# UNINSTALLING THE APPLICATION

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

➤ *To uninstall Kaspersky Mobile Security 9:*

1. Deactivate Privacy Protection (page [69](#)).
2. In the main window, switch to the applications window and select **Settings** → **Applications** → **Applications management**.
3. Select Kaspersky Mobile Security 9 from the list.

The **Application details** window opens.

4. Click **Delete**.

A confirm deletion window opens.

5. Confirm the deletion of Kaspersky Mobile Security 9, by clicking **OK**.

The application is deleted from the device.

6. On completion of the deletion, click **OK**.

# GETTING STARTED

This section contains information about how to start using Kaspersky Mobile Security 9: activate it, set the application's secret code, enable the secret code recovery function, recover the secret code and start the application.

## IN THIS SECTION

---

Activating the application.....	<a href="#">21</a>
Setting the secret code.....	<a href="#">24</a>
Enabling the option to recover the secret code .....	<a href="#">25</a>
Recovering the secret code.....	<a href="#">25</a>
Starting the application.....	<a href="#">26</a>
Viewing information about the application .....	<a href="#">26</a>

## ACTIVATING THE APPLICATION

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

The application can be activated if an Internet connection is set on the device, an operating SIM card is inserted and the PIN code is entered (if one is set). If these requirements are not fulfilled, it is not possible to activate the application.

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;
  - disabling Privacy Protection.

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, and it cannot be updated.

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, and the application databases are no longer updated.

**IN THIS SECTION**

---

Activating the commercial version ..... [22](#)

Activating the subscription for Kaspersky Mobile Security 9 ..... [23](#)

Purchasing an activation code online ..... [23](#)

Activating the trial version ..... [24](#)

**ACTIVATING THE COMMERCIAL VERSION**

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

1. Switch from the main window to the applications window.
2. Select **Kaspersky Mobile Security 9** and run the application.

This will open the **Activation** window.

3. Select **Enter activation code**.

This will open the **Enter activation code** window.

4. Subsequently enter the activation code received when purchasing the application and click **Activate**.

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. Go to setting the application secret code.

## ACTIVATING THE SUBSCRIPTION FOR KASPERSKY MOBILE SECURITY 9

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

1. Switch from the main window to the applications window.
2. Select **Kaspersky Mobile Security 9** and run the application.

This will open the **Activation** window.

3. Select **One-Click Buy**.
4. Read the information on activating your subscription and click **Activate**.

The application will check if the subscription service is accessible to the mobile service provider that you use. If the subscription service is accessible, information about the terms of subscription will be displayed on the screen.

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 with the subscription terms, return to the **Activation** window. 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. 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. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.

This will open the **Additional** window.

2. Select the item **License** → **Renewing the license**.

This will open the **Activation** window.

Select **Buy online**.

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

3. Press **Open**.

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

4. Follow the step-by-step instructions.
5. After completing the purchase of the activation code, switch to the activation of the application's commercial version activation.

## ACTIVATING THE TRIAL VERSION

➤ *To activate the trial version of Kaspersky Mobile Security 9:*

1. Switch from the main window to the applications window.
2. Select **Kaspersky Mobile Security 9** and run the application.

This will open the **Activation** window.

3. Select **Trial version**.
4. Confirm the trial version activation by clicking **Activate**.

The application will send a request to the Kaspersky Lab activation server and receive a license. Subsequently, the **About licensing** window opens with information about the application's license installed.

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 unauthorized access to the application's parameters.

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, Privacy Protection.

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

If you forget the application secret code, you can restore it (see the "Recovering the secret code" section on page [25](#)). For this purpose, the recovery of secret code option must be enabled in advance (see the "Recovering the secret code" section on page [25](#)).

➤ *To enter the secret code:*

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

The code entered is automatically verified.

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

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

The secret code is installed.

## ENABLING THE OPTION TO RECOVER THE SECRET CODE

After the first activation of the application, you may enable the option to recover the application's secret code. Then, in the future, you will be able to recover the secret code if it is forgotten.

If you decline to activate the function after the first activation of the application, you can enable it after reinstalling Kaspersky Mobile Security 9 on the device.

You can only recover the application secret code (see the "Recovering the secret code" section on page 25) if the recovery of secret code option is enabled. If you have forgotten your password and the secret code recovery function is disabled, it is impossible to use the functions of Kaspersky Mobile Security 9.

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

1. After installing the application's secret code (see section "Installing the secret code" on page 24) enter your e-mail address in the **Enable option to recover secret code** window.
2. Confirm activation of the secret code recovery function 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.

## 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 25).

➔ *To recover the application secret code:*

1. Switch from the main window to the applications window.
2. Select **Kaspersky Mobile Security 9**.

The **Kaspersky Mobile Security 9** window opens.

3. Click **Menu** → **Recover secret code**.

A message with the following information is displayed in the window:

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

4. Press **Go**.

Go to the website <http://mobile.kaspersky.com/recover-code> 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. Switch to the **Kaspersky Mobile Security 9** window.
7. Click **Menu** → **Enter recovery code** and enter the recovery code received.
8. Enter the new application secret code. To do this, enter a new application secret code in the fields **Enter new code** and **Confirm secret code**.
9. Click **Enter**.

## STARTING THE APPLICATION

➤ *To start Kaspersky Mobile Security 9:*

1. Switch from the main window to the applications window.
2. Select **Kaspersky Mobile Security 9**.
3. The **Kaspersky Mobile Security 9** window opens.
4. Enter the application secret code and press **OK**.

The application's main window opens.

## VIEWING INFORMATION ABOUT THE APPLICATION

You can view general information about Kaspersky Mobile Security 9 and its version.

➤ *To view information about the application:*

1. In the main Kaspersky Mobile Security 9 window, the **Additional** box opens.  
This will open the **Additional** window.
2. In the **Information** box, select **About**.

# MANAGING THE LICENSE

In the context of licensing Kaspersky Lab applications, it is important to know these terms below:

- License Agreement;
- license.

These terms are inseparably interlinked and constitute a single licensing pattern. Let us have a closer look at every term.

Furthermore, the section presents information about how to find information on the Kaspersky Mobile Security 9 license and extend the term of its validity.

## IN THIS SECTION

---

About the License Agreement .....	<a href="#">27</a>
About Kaspersky Mobile Security 9 licenses .....	<a href="#">27</a>
View License Information .....	<a href="#">28</a>
Renewing the license .....	<a href="#">29</a>

## ABOUT THE LICENSE AGREEMENT

The *License Agreement* is an agreement between a private individual or a legal entity which legally owns a copy of Kaspersky Mobile Security 9 and Kaspersky Lab. The agreement is included in every Kaspersky Lab application. It stated detailed information on the rights and limitations on using Kaspersky Mobile Security.

In accordance with the License Agreement, when purchasing and installing a Kaspersky Lab application, you obtain the unlimited right to owning its copy.

Kaspersky Lab also provides you with additional services:

- technical support;
- updating of Kaspersky Mobile Security 9 anti-virus databases;
- updating of Kaspersky Mobile Security 9 program modules.

In order to benefit, you must purchase and activate a license (see the "About Kaspersky Mobile Security 9 licenses" section on page [27](#)).

## ABOUT KASPERSKY MOBILE SECURITY 9 LICENSES

A *license* is the right to use Kaspersky Mobile Security 9 and the additional services associated with it as provided by Kaspersky Lab or its partners.

Every license has a validity period and type.

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

- technical support;

- updating of Kaspersky Mobile Security 9 anti-virus databases;
- updating of Kaspersky Mobile Security 9 program modules.

The scope of services provided depends on the license type.

The following license types are available:

- *Trial*—free license with a limited validity period, for example, 30 days, offered to get acquainted with Kaspersky Mobile Security 9.

The trial license can only be used once.

If you have a trial license, you can only contact Technical Support Service if your question is about activating the product or purchasing a commercial license. As soon as the Kaspersky Mobile Security 9 trial license expires, all features become disabled. To proceed with the application, you should activate it.

- *Commercial*—paid license with a limited validity period (for example, one year), provided upon purchase of Kaspersky Mobile Security 9.

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

On termination of the validity period of the commercial license, some functions of Kaspersky Mobile Security 9 become inaccessible, and the application databases will not be updated. One week before the license expiration date, the application will notify you of this event so you could renew the license in advance.

- *Commercial with subscription* – paid license with an option to renew it in automatic or manual mode. A license with subscription is distributed by service providers.

The subscription is valid for a limited period (30 days). After the subscription expires, it can be renewed manually or automatically. Method of renewing the subscription depends on the legislation and mobile service provider. The subscription is renewed automatically subject to timely prepayment to the provider.

In this case, the fixed amount specified in the terms of subscription is debited 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 subscription is not renewed, Kaspersky Mobile Security 9 stops updating the application databases, and the application's functionality becomes limited.

When using the subscription, you can activate the commercial license with an activation code. In this case, the subscription will be canceled automatically.

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

## 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. In the main Kaspersky Mobile Security 9 window, the **Additional** box opens.

This will open the **Additional** window.

2. Select **License** → **About license**.

## 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.

The application can be activated if an Internet connection is set on the device, an operating SIM card is inserted and the PIN code is entered (if one is set). If these requirements are not fulfilled, it is not possible to activate the application.

### IN THIS SECTION

Renewing the license with the activation code.....	<a href="#">29</a>
Renewing the license online.....	<a href="#">30</a>
Renewing the license by activating a subscription .....	<a href="#">30</a>
Unsubscribing .....	<a href="#">31</a>
Renewing the subscription .....	<a href="#">31</a>

## RENEWING THE LICENSE WITH THE ACTIVATION CODE

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

1. In the main Kaspersky Mobile Security 9 window, the **Additional** box opens.

This will open the **Additional** window.

2. Select the item **License** → **Extend license**.

This will open the **Activation** window.

3. Select **Enter activation code**.

This will open the **Enter activation code** window.

4. Subsequently enter the activation code received and click **Activate**.

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.

## RENEWING THE LICENSE ONLINE

➔ *To renew your license online:*

1. In the main Kaspersky Mobile Security 9 window, the **Additional** box opens.

This will open the **Additional** window.

2. Select the item **License** → **Extend license**.

This will open the **Activation** window.

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 can buy an activation code online.

5. Follow the step-by-step instructions.

6. When the order to renew the license is processed, enter the activation code obtained (see the "License renewal with activation code" section on page [29](#)).

## RENEWING THE LICENSE BY ACTIVATING A SUBSCRIPTION

You can renew the term of the license by activating subscription (see section "On licensing Kaspersky Mobile Security 9" on page [27](#)) on 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:*

1. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.

This will open the **Additional** window.

2. Select the item **License** → **Extend license**.

This will open the **Activation** window.

Select **One-Click Buy**.

3. Read the subscription information and click **Activate**.

The application will check if the subscription service is accessible to the mobile service provider that you use. If the subscription service is accessible, information about the terms of subscription will be displayed on the screen.

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.

4. 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 with the subscription terms, return to the **Activation** window. The application will cancel the subscription activation and switch back to the screen on which you can select another method of renewing the license.

## 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 [31](#)).

➤ *To cancel a subscription to Kaspersky Mobile Security 9:*

1. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.
2. This will open the **Additional** window.
3. Select **Unsubscribe**.
4. 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.

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. In the main Kaspersky Mobile Security 9 window, the **Additional** box opens.  
This will open the **Additional** window.
2. Select the item **License** → **Extend license**.  
This will open the **Activation** window.
3. Select **One-Click Buy**.

If the term of validity of the current license has expired, Kaspersky Mobile Security 9 suggests activating the subscription (see section "About Kaspersky Mobile Security 9 licenses" on page [27](#)).

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.

# APPLICATION INTERFACE

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

## IN THIS SECTION

Protection status window.....	<a href="#">32</a>
Home screen widget .....	<a href="#">33</a>

## PROTECTION STATUS WINDOW

After starting the program, the application's main window opens (see Figure below).

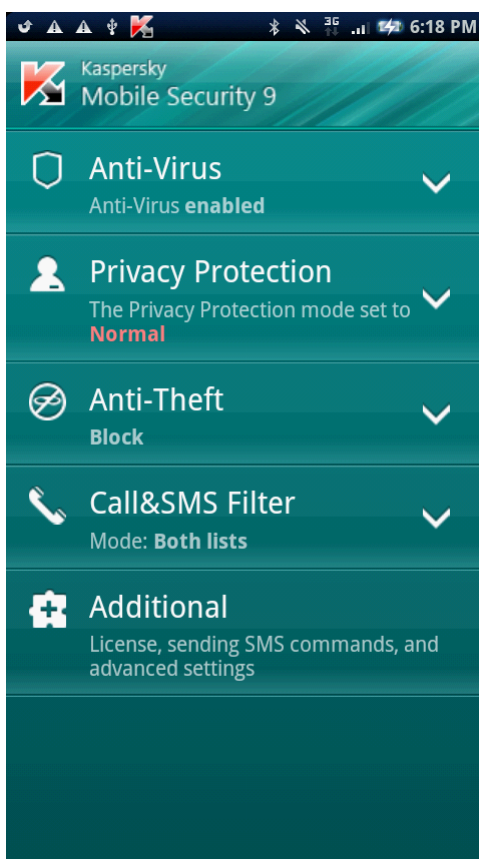


Figure 1. The application's main window

The expanding modules are located in the main window. Every module allows switching to the settings of the parameters of one of the application's components and fulfilling protection tasks.

The main window also displays the condition of its main components.

For every module, the following information is displayed below its name:

- **Anti-Virus** – status of device protection from viruses and other malicious applications (see section "File system protection" on page [34](#));

- **Privacy Protection** – confidential information hiding mode.
- **Anti-Theft** – Anti-Theft functions statuses.
- **Call&SMS Filter** – filtering mode for calls and SMS.
- **Additional** – information on additional parameters grouped in this module (see section "Making additional settings" on page [80](#)).

## HOME SCREEN WIDGET

When using Kaspersky Mobile Security 9, the home screen widget is accessible to you. After installing the application, the widget automatically appears in the device's main window (see Figure below).



Figure 2. Home screen widget

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

The following color indication is presented:

- if the protection is green, protection is enabled;
- if protection is gray, protection is disabled;
- a green background color means that confidential information is hidden;
- a gray background color means that confidential information is displayed;
- an exclamation mark in a yellow triangle means that the license's term of validity has expired or that the license has not been installed.

# FILE SYSTEM PROTECTION

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

## IN THIS SECTION

---

About Protection.....	<a href="#">34</a>
Activate/Deactivate Protection .....	<a href="#">34</a>
Configuring the protection area .....	<a href="#">36</a>
Selecting the action to be performed on detected objects.....	<a href="#">36</a>

## ABOUT PROTECTION

Protection starts when operation system starts up and is always found in the device's memory. Protection checks all open, saved and started files (including those on memory cards) as well as installed applications.

Files are scanned according to the following algorithm:

1. Protection scans every file when the user accesses it.
2. Protection analyses the file for the presence of malicious objects. Malicious objects are detected by comparison with the application's anti-virus databases. The anti-virus databases contain descriptions of all currently known malicious objects, and methods for neutralizing them.
3. According to the analysis results, the following types of Protection are possible:
  - if malicious code is detected in the file, protection performs an action in accordance with the settings made (see section "Selection of action in respect of objects detected" on page [36](#));
  - If no malicious code is discovered in the file, it will be immediately restored.

Protection checks the installed application for viruses when it is run for the first time. Protection performs a scan on the grounds of the antivirus databases. If protection detects a virus during while scanning an application, it suggests deleting the application.

## ACTIVATE/DEACTIVATE PROTECTION

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

To ensure protection from viruses and other threats, resources of the device are used. In order to reduce the load on the device when executing several tasks, you can temporarily stop Protection.

**The Kaspersky Lab specialists recommend that you do not disable Protection, since this could lead to the infection of your computer and data loss.**

Deactivating protection has no impact on performing antivirus scan tasks and updating the application's antivirus databases.

The current status of protection is displayed in the application's main window in the **Anti-Virus** model.

➤ *To enable Protection:*

1. In the main Kaspersky Mobile Security 9 window, the **Anti-Virus** box opens.
2. Click **Additional**.

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

3. Check the **Enable Protection** box (see Figure below).



Figure 3. Enabling Protection

➤ *To disable Protection:*

1. In the main Kaspersky Mobile Security 9 window, the **Anti-Virus** box opens.
2. Click **Additional**.

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

3. Uncheck the **Enable Protection** box.

## CONFIGURING THE PROTECTION AREA

By default, Kaspersky Mobile Security 9 scans all file types. You can select files for Kaspersky Mobile Security 9 to check for the presence of malicious objects during its Protection operation.

Before setting protection, first ensure that protection is enabled.

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

1. In the main Kaspersky Mobile Security 9 window, the **Anti-Virus** box opens.

2. Click **Additional**.

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

3. Select **Protection settings** → **Type of files for protection**.

4. Select the value for the settings of the **Type of files for protection**:

- **All files** - scan all types of files.
- **Executable files** – scan only executable application files (for example, files of the formats EXE, MDL, APP, DLL, SO, ELF).

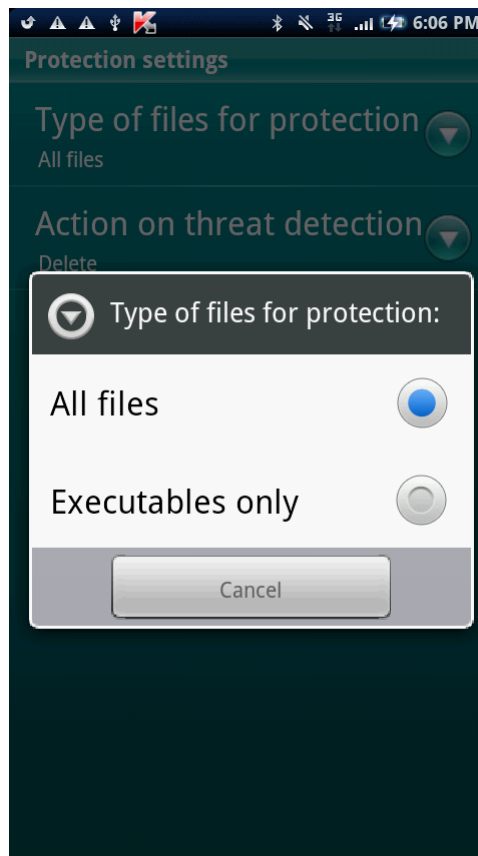


Figure 4. Selecting the objects to scan

## SELECTING THE ACTION TO BE PERFORMED ON DETECTED OBJECTS

By default, Kaspersky Mobile Security 9 deletes the detected threat. You can choose the action that Kaspersky Mobile Security 9 performs when it detects a malicious object.

➤ To set the application's response when detecting a threat, proceed as follows:

1. In the main Kaspersky Mobile Security 9 window, the **Anti-Virus** box opens.
2. Click **Additional**.

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

3. Select **Protection settings** → **Action on threat detection**.
4. Set an action which the application takes if it finds a malicious object. To do this, select a value for the settings of the **Action on threat detection** (see Figure below):
  - **Delete** - delete malware objects without notifying the user.
  - **Skip** – skip malicious objects. Block the object when attempts are made to use it (for instance, copy or open).

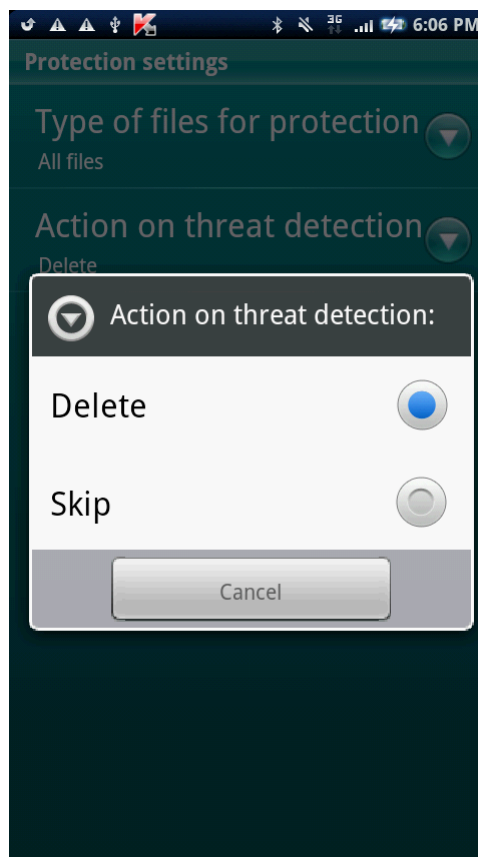


Figure 5. Selecting the action on threat detection

# SCANNING THE DEVICE

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

## IN THIS SECTION

---

About scanning the device .....	<a href="#">38</a>
Starting a scan manually .....	<a href="#">38</a>
Starting a scheduled scan .....	<a href="#">40</a>
Selection of object type to be scanned.....	<a href="#">40</a>
Configuring archive scans .....	<a href="#">41</a>
Selecting the action to be performed on detected objects.....	<a href="#">42</a>

## ABOUT SCANNING THE DEVICE

Scan device on demand helps detect and remove threats on your device. Kaspersky Mobile Security 9 allows performing a full or partial scan of the device included – i.e. scan only the content of the device's built-in memory or a specific folder (including that located on the storage card).

The device is scanned as follows:

1. Kaspersky Mobile Security 9 scans the file types set (see "Selecting the object types to be scanned" section on page [40](#)).
2. During the scan, each file is analyzed for the presence of malicious objects (malware). Malicious objects are detected by comparison with the application's anti-virus databases. Anti-Virus databases contain descriptions of all known malicious objects, and methods for neutralizing them.

If following a file analysis the application detects malicious code, it performs the action selected in accordance with the settings made (see section "Selection of action in respect of objects detected" see page [42](#)).

The scan starts manually or automatically in accordance with a schedule (see "Starting a scheduled scan" on page [40](#)).

## STARTING A SCAN MANUALLY

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

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

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Virus** module.
2. Select **Start scan**.
3. Select the device scan area (see Figure below):
  - **Full scan** – scan the device's entire file system. By default, the application scans files saved to the device's onboard memory and memory cards.

- **Folder scan** - scan a separate object in the device's file system or on the storage card. When **Folder scan** is selected, a window displaying the device's **File system** will open. To start scanning a folder, select the folder required and click on the scan icon located to the right of the folder.
- **Memory scan** - scan the processes started in the system memory and its corresponding files.

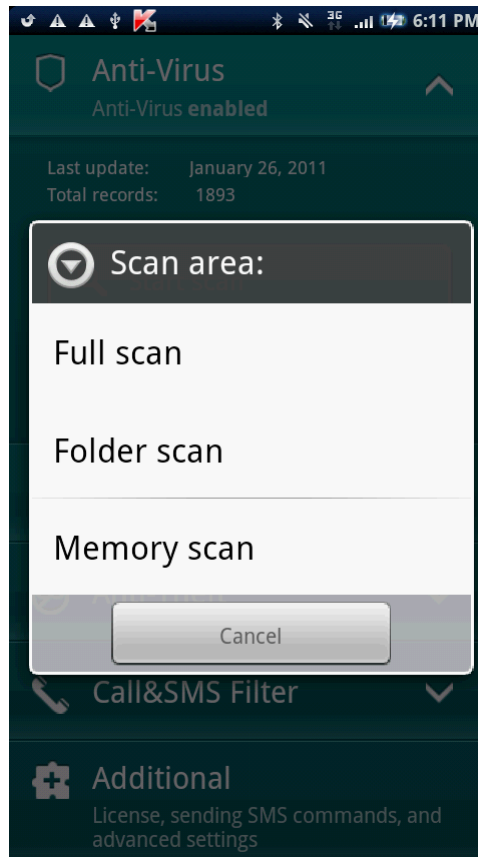


Figure 6. Selecting the scan area

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

If Kaspersky Mobile Security 9 detects a malicious object, it performs an action in accordance with the scan parameters set (see the "Selecting an action to be performed on objects" section on page [42](#)).

By default, if Kaspersky Mobile Security 9 detects a threat, it attempts to eliminate it. If disinfection fails is impossible, the application deletes the malicious object.

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

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

## STARTING A SCHEDULED SCAN

You can set the file system scan to start automatically on schedule. A scheduled scan is carried out in background mode. When a malicious object is detected, the action selected in the scan settings will be performed on it (see "Selecting an action to be performed on objects" section on page [42](#)).

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

➤ *To set a scan schedule:*

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Virus** module.
2. Click **Additional**.

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

3. Select the **Scan settings**.

The **Scan settings** window opens.

4. Select the scan start mode. To do this, set the value for the **Scheduled scan settings**:
  - **Weekly** – perform the scan once a week. To do this, set the day and start time of the scan. To do this, select values for the settings **Scan day** and **Scan time**.
  - **Daily** – perform the scan every day. To do this, set the start time of the scan. Set the value for the **Scan time** setting.
  - **Disabled** – disable scheduled scans.

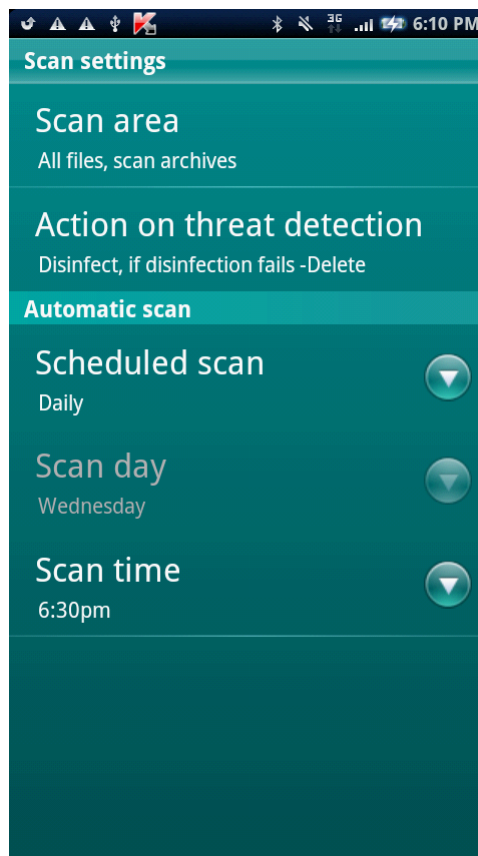


Figure 7. Configure automatic scan

## SELECTION OF OBJECT TYPE TO BE SCANNED

By default, Kaspersky Mobile Security 9 scans all files saved on the device and storage card. To shorten the scan time, you can select the object type to be scanned, i.e. determine which file formats the application should scan for malicious code.

➔ *To select objects to be scanned:*

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Virus** module.
2. Click **Additional**.

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

3. Select **Scan settings** → **Scan area**.

The **Scan area** window opens.

4. Set the value for the setting **Type of files** (see Figure below):

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

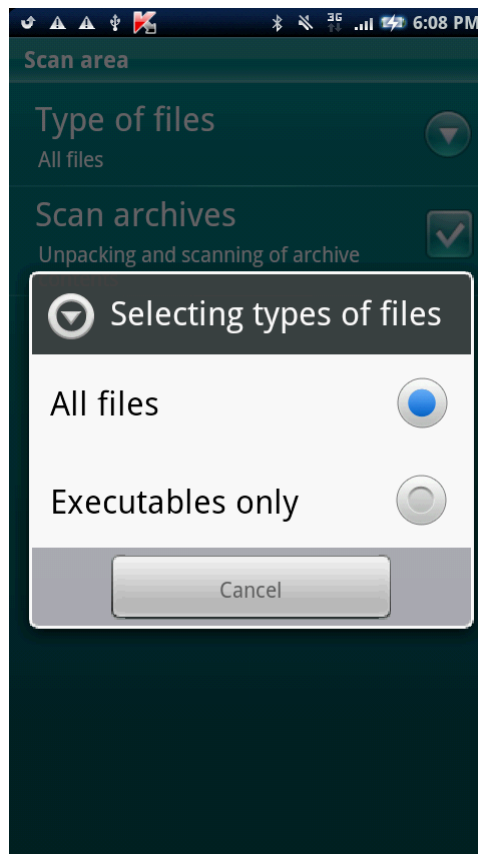


Figure 8. Selecting types of files to scan

## CONFIGURING ARCHIVE SCANS

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

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

➔ *To enable scan of archives:*

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Virus** module.
2. Click **Additional**.

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

3. Select **Scan settings** → **Scan area**.

The **Scan area** window opens.

4. Select the **Scan archives** check box.

## SELECTING THE ACTION TO BE PERFORMED ON DETECTED OBJECTS

By default, Kaspersky Mobile Security 9 tries to rectify a threat on detection, if disinfection fails, it deletes it. You can set the actions of the application when a threat is detected.

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

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Virus** folder.
2. Click **Additional**.

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

3. Select **Protection settings** → **Action on threat detection**.

The **Action on threat detection** window opens.

4. Set the first action in respect of a threat detected. Set the **Disinfect**, check box in order for the application to first attempt to disinfect the detected threat. Remove the **Disinfect** check box in order for the application not to attempt to disinfect the detected threat.
5. Set the second action of the application if a detected threat cannot be disinfected. To do this, select the value for the setting **If it is not possible to disinfect** (see Figure below):

- **Delete**: delete malware objects without notifying the user.
- **Ask user** - prompt the user for actions when a malicious object is detected.
- **Skip** – do not process malware objects and record information about their detection in the application's log. Block the object when attempts are made to use it (for instance, copy or open).



Figure 9. Selecting an action with malicious objects, if they cannot be disinfected

# 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.....	<a href="#">44</a>
About Call&SMS Filter modes.....	<a href="#">45</a>
Changing the Call&SMS Filter mode.....	<a href="#">45</a>
Creating the Black List.....	<a href="#">46</a>
Creating a White List.....	<a href="#">49</a>
Responding to SMS messages and calls from contacts not in the phone book.....	<a href="#">52</a>
Responding to SMS messages from non-numeric numbers.....	<a href="#">53</a>
Selecting a response to incoming SMS.....	<a href="#">54</a>
Selecting response to incoming calls.....	<a href="#">55</a>
Viewing Log records.....	<a href="#">56</a>

## 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 [45](#)). 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 on blocked SMS and calls is logged in the Call&SMS filter log (see section "Viewing entries in the log" on page [56](#)).

## 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 [45](#)). The current Call&SMS Filter mode is displayed on the **Call&SMS Filter** tab next to the **Mode** menu item.

## CHANGING THE CALL&SMS FILTER MODE

➔ *To change the Call&SMS Filter mode, proceed as follows:*

1. In the main window of Kaspersky Mobile Security 9 open the **Call&SMS Filter** module.
2. Select **Mode: <current component mode>**.

The **Call&SMS Filter** window opens.

3. Select the value for the setting **Call&SMS Filter mode** (see Figure below).

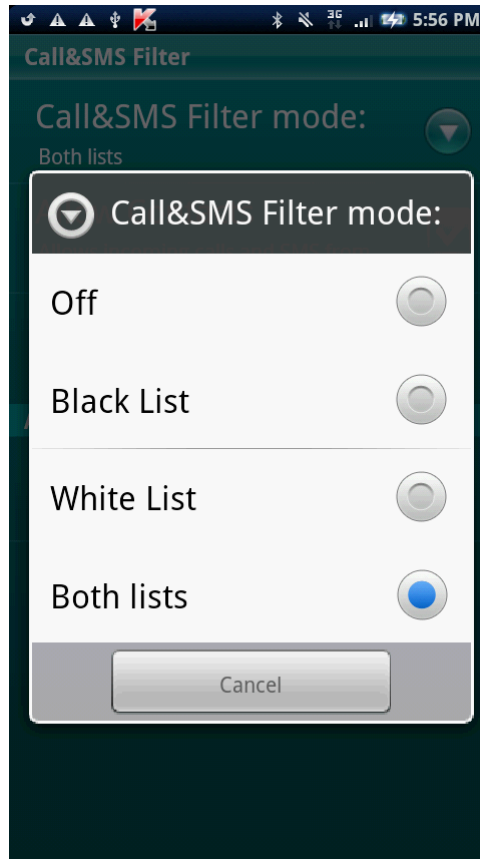


Figure 10. Changing the Call&SMS Filter mode

## 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 on blocked SMS and calls is logged in theC all&SMS filter log (see section "Viewing entries in the log" on page 56).

**IN THIS SECTION**

Adding entries to the Black List ..... [47](#)

Editing entries in the Black List ..... [48](#)

Deleting entries from the Black List ..... [49](#)

## 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. In the main window of Kaspersky Mobile Security 9 open the **Call&SMS Filter** module.

2. Select **Black List**.

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

3. Click **Add**.

4. Set values with the following 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.
- **Blocked 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.
- **Blocked 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.

Setting accessible for **SMS only** events.

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

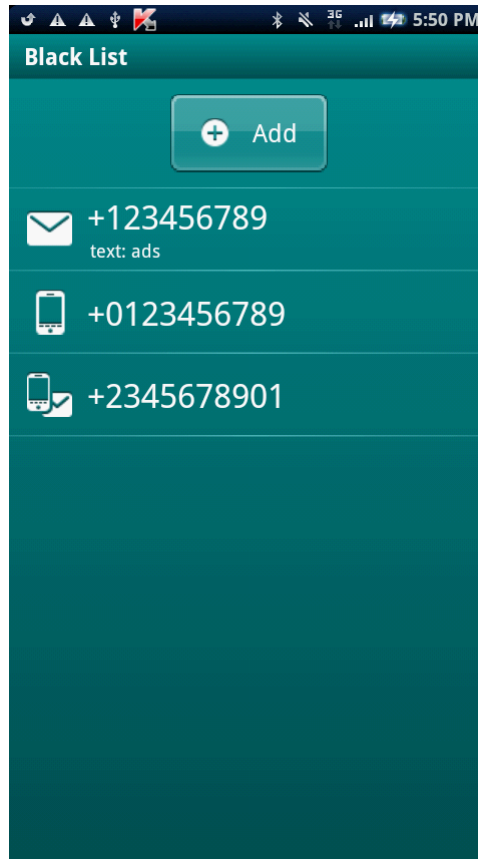


Figure 11. Adding entries to the Black List

## EDITING ENTRIES IN THE BLACK LIST

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

➔ *To edit an entry in the Call&SMS Filter Black List:*

1. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **Black List**.

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

3. Select an entry from the list which you wish to change and select **Change** in the context menu for the entry.
4. Change the necessary settings:

- **Blocked 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.
- **Blocked 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.

Setting accessible for **SMS only** events.

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

## 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. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **Black List**.  
This will open the **Black List** window.
3. Select an entry in the list which is to be deleted and select **Delete** for the entry in the context menu.  
The confirmation window opens.
4. Confirm the uninstalling by pressing the **Yes** button.

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

1. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **Black List**.  
This will open the **Black List** window.
3. Select **Delete all** in the context menu.  
The confirmation window opens.
4. Confirm the uninstalling by pressing the **Yes** button.

The list is emptied.

## CREATING A WHITE LIST

The White List contains entries of allowed numbers, i.e., numbers from which 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..... [50](#)

Editing entries in the White List ..... [51](#)

Deleting entries from the White List ..... [52](#)

## 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. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.

2. Select **White List**.

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

3. Click **Add** (see Figure below).

4. Apply the following settings for the new entry:

- **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.
- **Permitted phone number:** key phrase indicating that the received SMS message is wanted. 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.
- **Permitted 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.

Setting accessible for **SMS only** events.

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

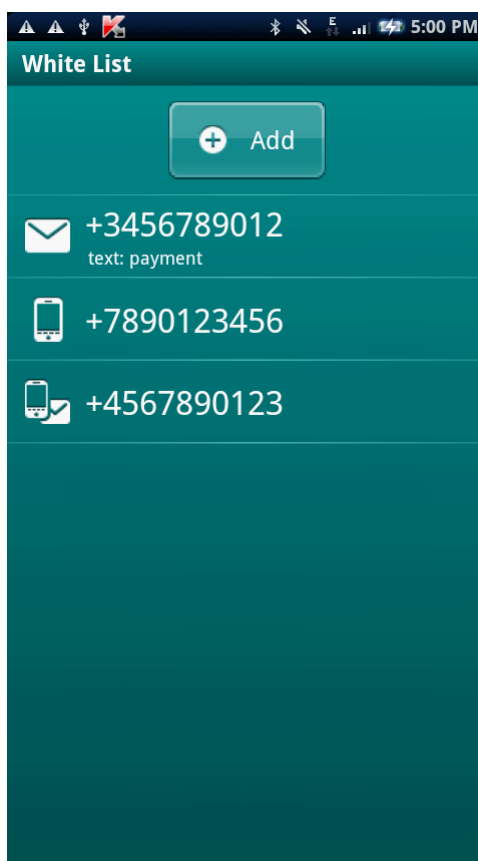


Figure 12. Adding an entry to the White List

## EDITING ENTRIES IN THE WHITE LIST

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

➔ *To edit an entry in the Call&SMS Filter White List:*

1. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **White List**.  
This will open the **White List** window.
3. Select an entry in the list which is to be deleted and select **Change** for the entry in the context menu.
4. Change the necessary settings:
  - **Permitted phone number** - phone 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.
  - **Permitted 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.

Setting accessible for **SMS only** events.

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

## 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. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **White List**.  
  
This will open the **White List** window.
3. Select an entry in the list which is to be deleted and select **Delete** for the entry in the context menu.  
  
The confirmation window opens.
4. Confirm the uninstalling by pressing the **Yes** button.

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

1. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **White List**.  
  
This will open the **White List** window.
3. Select **Delete all** in the context menu.  
  
The confirmation window opens.
4. 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 Call&SMS Filter modes **Both lists** or **White List** are selected, you can additionally set an Call&SMS Filter response to SMS messages and calls from subscribers whose numbers are not contained 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. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **Mode: <current component mode>**.  
  
The **Call&SMS Filter** window opens.
3. Select the value for the **Allow Contacts** setting (see Figure below):
  - for Anti-Spam 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, check the **Allow Contacts** checkbox.

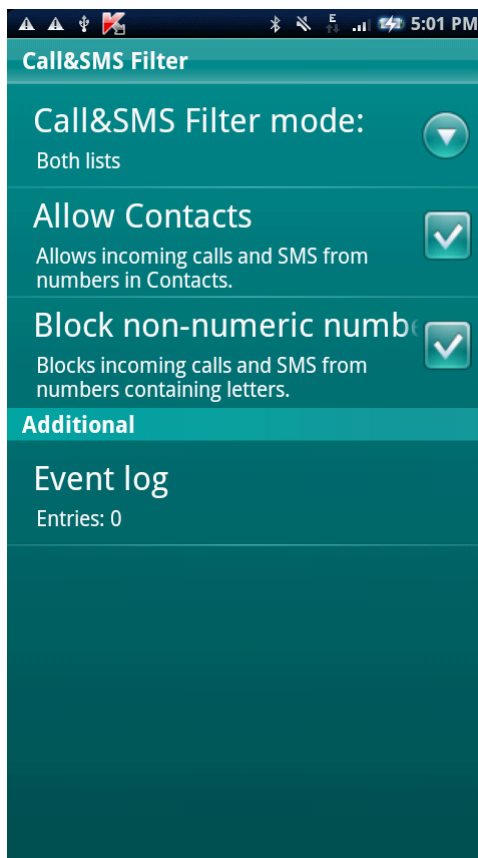


Figure 13. Reaction of Call&SMS Filter to numbers not in Contacts

## RESPONDING TO SMS MESSAGES FROM NON-NUMERIC NUMBERS

For the Call&SMS Filter mode **Both lists** or **White List**, you can additionally expand the Black List by including in it all non-numerical numbers (containing letters). In this event, the Call&SMS Filter processes SMS and non-numerical numbers like numbers from the Black List.

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

1. In the main window of Kaspersky Mobile Security 9, open the **Call&SMS Filter** module.
2. Select **Mode: <current component mode>**.

The **Call&SMS Filter** window opens.

3. Select the value for the **Block non-numeric numbers** setting (see Figure below):
  - for the Call&SMS Filter to block non-numerical numbers, check the **Blocking non-numerical numbers** check box;
  - for the Call&SMS Filter to filter out SMS from non-numerical numbers on the basis of the Call&SMS Filter mode set, remove the **Blocking non-numerical numbers** checkbox.

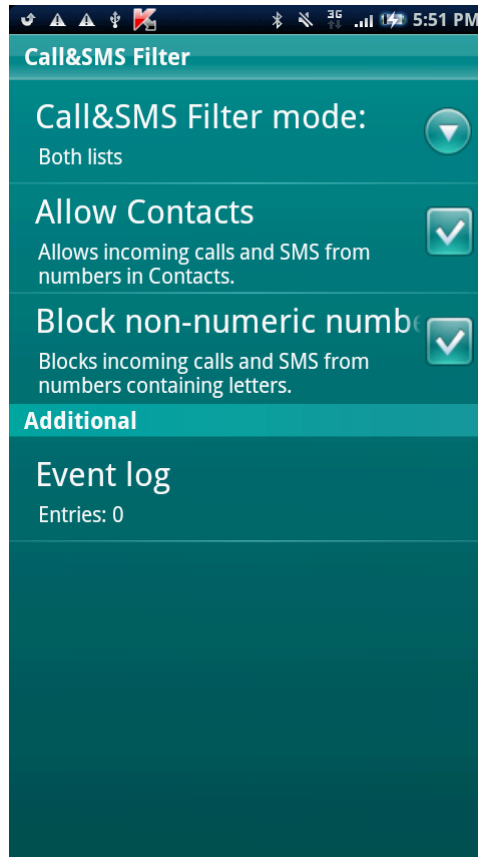


Figure 14. Selecting an action for Call&SMS Filter to perform when receiving an SMS from non-numeric number

## SELECTING A RESPONSE TO INCOMING SMS

Call&SMS Filter checks incoming SMS against the Black and White lists in the **Both lists** mode.

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 SMS and add a telephone number to the Black List, click **Block**.
- To deliver SMS and add a sender's telephone number to the White List, click **Allow**.
- To deliver the SMS message without adding the sender's telephone number to either list, press **Skip**.

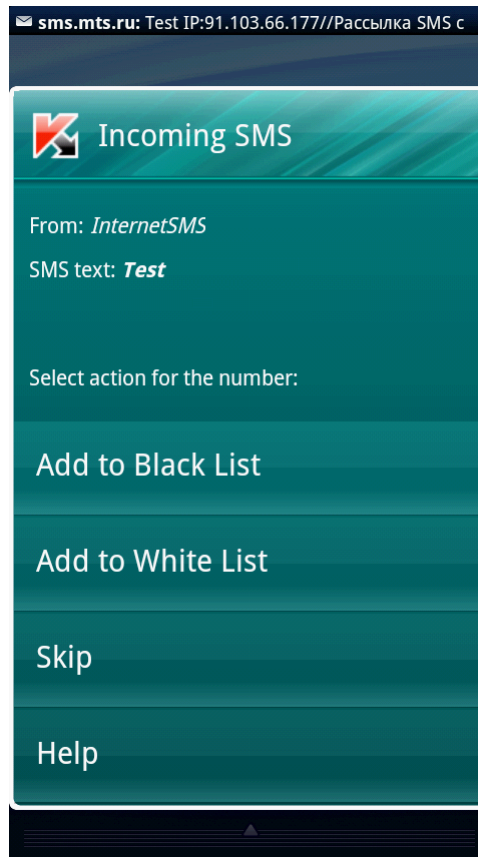


Figure 15. Call&SMS Filter notification about an accepted SMS

Information on blocked SMS and calls is logged in the Call&SMS filter log (see section "Viewing entries in the log" on page [56](#)).

## SELECTING RESPONSE TO INCOMING CALLS

Call&SMS Filter checks incoming SMS against the Black and White lists in the **Both lists** mode. 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 a caller's telephone number to the Black List, click **Block**.
- To add a caller's telephone number to the White List, click **Allow**.
- If you don't want to add the caller's number to either list, press **Skip**.

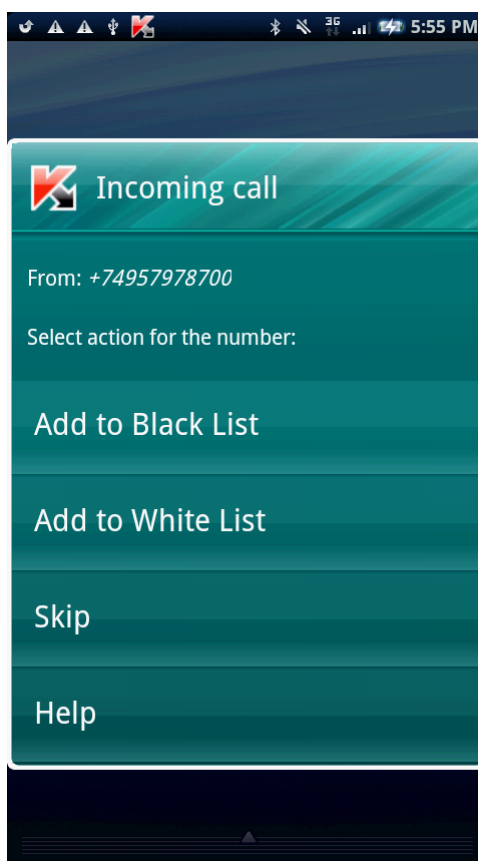


Figure 16. Call&SMS Filter notification about an accepted received call

Information on blocked SMS and calls is logged in the Call&SMS filter log (see section "Viewing entries in the log" on page 56).

## VIEWING LOG RECORDS

You can view information on blocked calls and SMS in the Call&SMS Filter log. Entries in the log are sorted in reverse chronological order.

The following information is provided for every entry:

- telephone number, from which the event was blocked by the Call&SMS Filter;
- blocking date;
- blocking time.

➔ To view information on the blocked calls and SMS, proceed as follows:

1. In the main window of Kaspersky Mobile Security 9, open the module **Call&SMS Filter**.
2. Select **Mode: <current component mode>**.  
The **Call&SMS Filter** window opens.
3. Click on the **Additional** module **Event log**.

The **Call&SMS Filter log** window opens.

- ➡ *To view detailed information on the blocked event,*  
select the relevant entry in the log

# 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 .....	<a href="#">58</a>
Blocking the device .....	<a href="#">59</a>
Deleting personal data .....	<a href="#">60</a>
Creating a list of folders to delete.....	<a href="#">62</a>
Monitoring the replacement of a SIM card on the device .....	<a href="#">63</a>
Determining the device's geographical coordinates .....	<a href="#">65</a>
Starting Anti-Theft functions remotely .....	<a href="#">67</a>

## 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** – the Data Wipe function allows you to delete the following personal data from the device remotely: Contacts and SIM card entries, SMS, call log, calendar, Internet connection settings, user accounts (except Google accounts), as well as files from the list of folders to be deleted.

*Kaspersky Mobile Security 9 only deletes contacts on the SIM card on devices with version 2.0 or above of the Android operating system.*

- **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 (see "Remote start of the Anti-Theft functions" on page [67](#)).

To remotely start the Anti-Theft functions, you must know the application's secret code that was set on the first start of Kaspersky Mobile Security 9 of the device, to which the SMS command is sent.

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

## BLOCKING THE DEVICE

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

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

➔ To enable the Block function:

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Theft** module.
2. Click **Block: <current function status>**.

This will open the **Block** window.

3. Check the **Enable Block** box.
4. Enter the message which is displayed on the device's screen in blocked mode in the **Test 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.

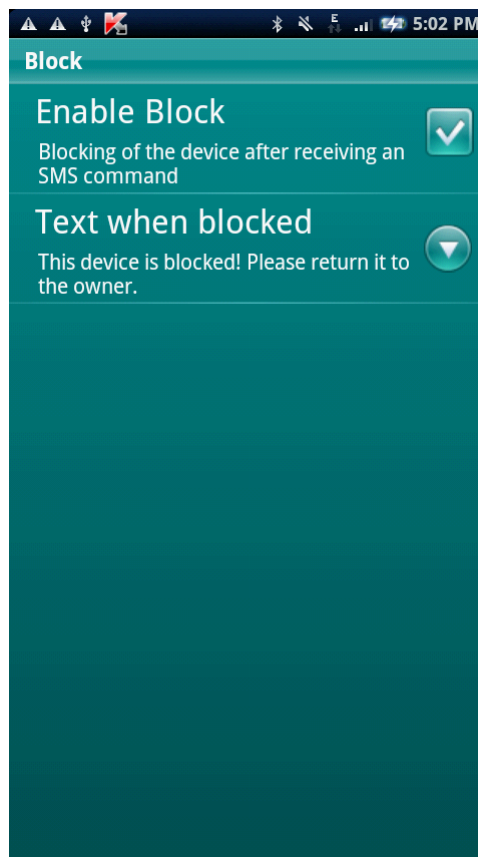


Figure 17. Block function settings

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

- Use a Kaspersky Lab mobile application, such as Kaspersky 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. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.  
This will open the **Additional** window.
2. Select **Send SMS command**.
3. For the **Select SMS command** setting, select **Block**.
4. In the **Phone number receiving the SMS command** field, enter the telephone number of the device receiving the SMS command.
5. In the **Secret code of the device receiving the SMS command** field, enter the application's secret code stated on the device receiving the SMS command.
6. Press **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:

- personal details of the user (entries in Contacts and on the SIM card, SMS, calls log, calendar, Internet connection settings, login entries with the exception Google login entry);
- files from the list of objects for deletion (see the "Creating a list of folders to delete" section on page [62](#)).

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. In the main window of Kaspersky Mobile Security 9, open the **Anti-Theft** folder.
2. Click **Data Wipe: <current function status>**.  
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 desired settings in the **Information to be deleted** block (see Figure below):

- to delete personal data, check the **Personal data** box;
- to delete files from the list of folders for deletion, set the check box **Folders** and go to creation of list for deletion (see section "Creation of list of folders to be delete" on page [62](#)).

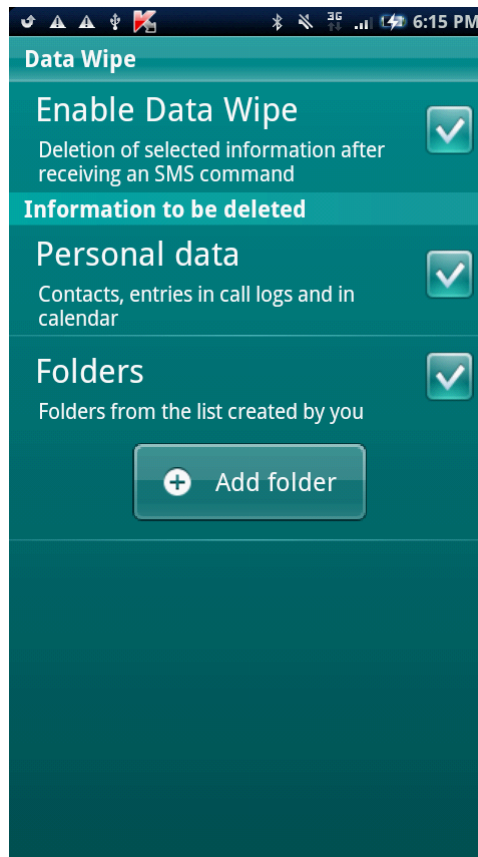


Figure 18. Data Wipe function settings

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

- Use a Kaspersky Lab mobile application, such as Kaspersky 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. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.

This will open the **Additional** window.

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

To enable Anti-Theft to delete all folders from the list after a special SMS message is received, make sure that the **Folders** box is checked in the Data Wipe settings.

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

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Theft** folder.
2. Click **Data Wipe**.  
  
This will open the **Data Wipe** screen.
3. Click **Add** (see Figure below).

The **Folder selection** window opens.

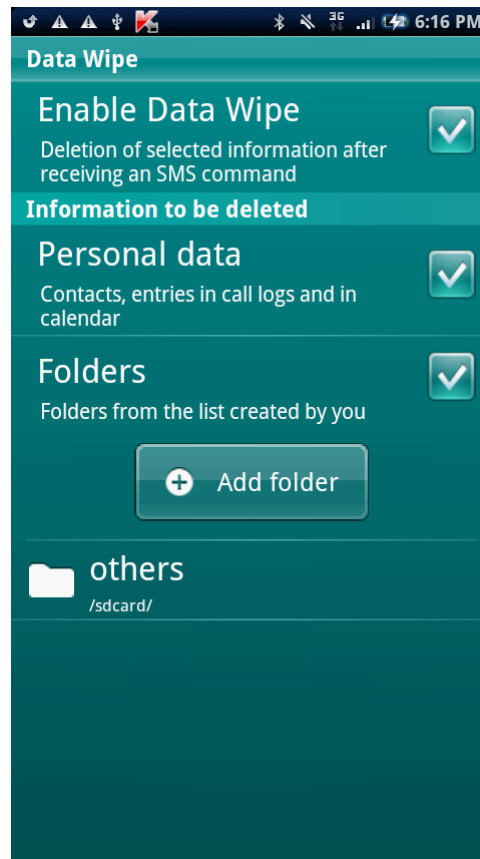


Figure 19. Adding a folder

4. Select the folder required by clicking on the icon to the right of the folder's name.

The folder is added to the list of folders for deletion located below the **Folder** settings

➡ *To remove a folder from the list:*

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Theft** module.
2. Click **Data wipe**.

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

3. Go to the list of objects for deletion.
4. Select a folder from the list and click **Delete folder** in the context menu.

The confirmation window opens.

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

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

## MONITORING THE REPLACEMENT OF A SIM CARD ON THE DEVICE

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

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

1. In the main window of Kaspersky Mobile Security 9, the **Anti-Theft** module opens.

2. Click **SIM Watch: <current component status>**.

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

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

4. To check the replacement of the SIM card on the device, make the following settings:

- To automatically receive SMS using the number of your telephone, enter a telephone number to which the SMS is sent in the **Send new number** module for the **Phone number** setting.

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

- To receive an e-mail with the new telephone number, in the **Send new number** module enter an e-mail address for the **E-mail address** setting.
- 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 the message on the screen in blocked status, enter the message text in the **Additional** module for the **Text when blocked** setting.

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

The setting is accessible if the **Block** checkbox is checked.

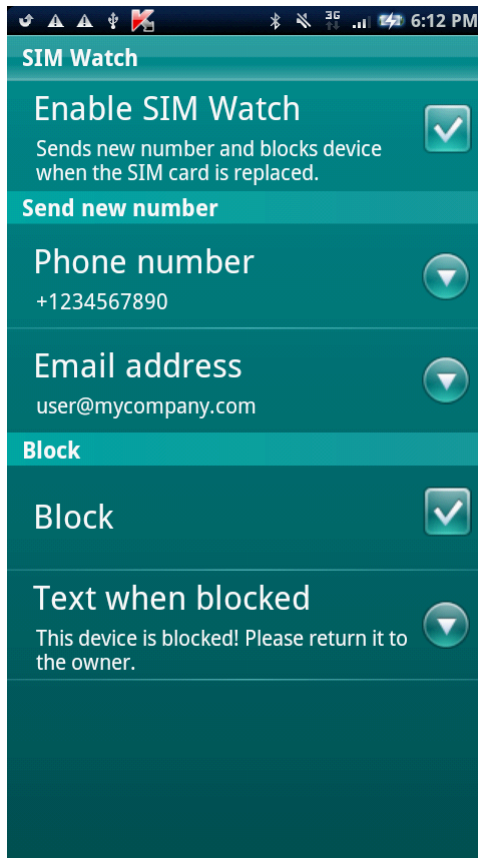


Figure 20. SIM Watch function settings

## 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.

If a GPS receiver is installed on the device, it activates automatically after the device receives a special SMS command. If the GPS Find function cannot obtain the device's coordinates with the use of GPS, it determines the device's approximate coordinates on the basis of base stations.

➔ To enable the GPS Find function:

1. In the main window of Kaspersky Mobile Security 9, open the **Anti-Theft** folder.
2. Click **GPS Find: <current component status>**.  
This will open the **GPS Find** window.
3. Check the **Enable GPS Find** box.

When receiving a special SMS command, Kaspersky Mobile Security 9 automatically sends the device's coordinates in a reply SMS to the number from which the SMS command was sent.

4. To also receive the device's coordinates by e-mail, enter an e-mail address in the **Send device coordinates** module for the **E-mail address** settings (see Figure below).

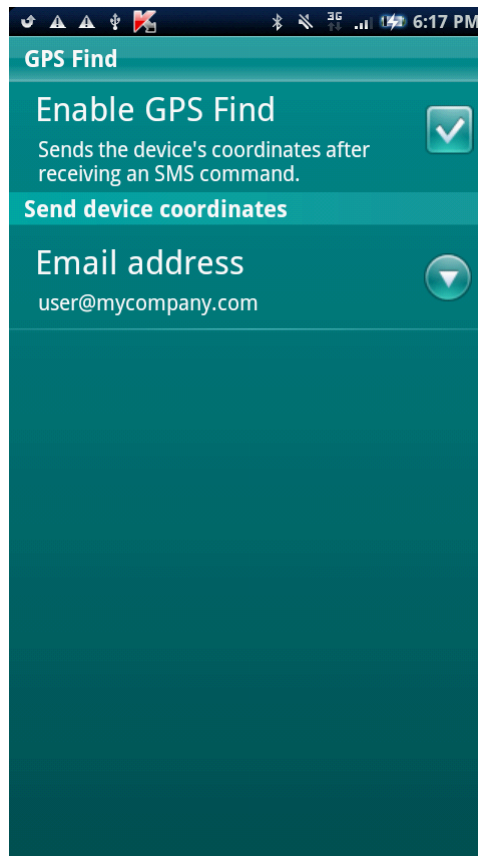


Figure 21. GPS Find function settings

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

- Use a Kaspersky Lab mobile application, such as Kaspersky 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. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.

This will open the **Additional** window.

2. Click **Send command**.
3. Select the **GPS Find** value for the **Select SMS command** setting.
4. In the **Phone number receiving the SMS command** field, enter the telephone number of the device receiving the SMS command.
5. In the **Secret code of the device receiving the SMS command** field, enter the application's secret code stated on the device receiving the SMS command.
6. Press **Send**.

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

send an SMS to the other device; the message should contain the text `hide:<code>` where `<code>` is the secret code of the application set on the other 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. In the main window of Kaspersky Mobile Security 9, expand the **Additional** module.
2. Select the function for remote launch on another mobile device. To do this, select one of the proposed values for the **Select SMS command** setting:
  - **Block;**
  - **Data Wipe;**
  - **GPS Find.**
  - **Privacy Protection.**

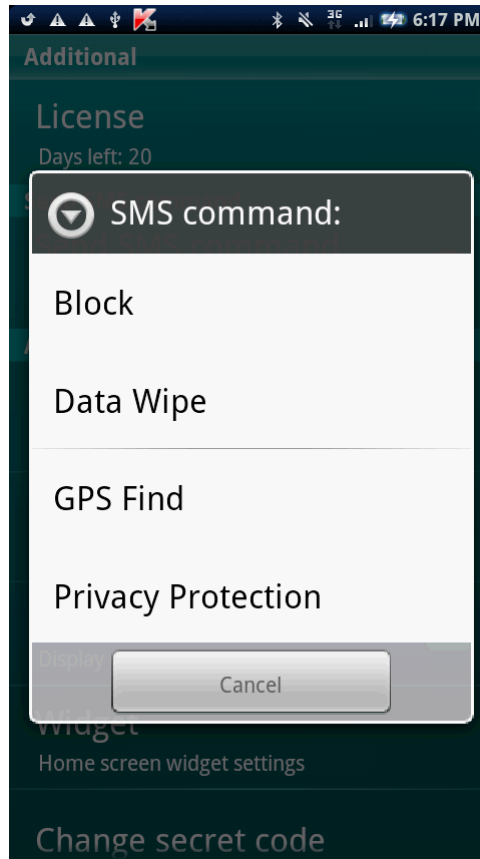


Figure 22. Remote start of Anti-Theft and Privacy Protection functions

3. In the **Phone number receiving the SMS command** field, enter the telephone number of the device receiving the SMS command.
4. In the **Secret code of the device receiving the SMS command** field, enter the application's secret code stated on the device receiving the SMS command.
5. Press **Send**.

# PRIVACY PROTECTION

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

## IN THIS SECTION

---

Privacy Protection .....	<a href="#">69</a>
Privacy Protection modes.....	<a href="#">69</a>
Enabling/disabling Privacy Protection .....	<a href="#">70</a>
Enabling Privacy Protection automatically.....	<a href="#">70</a>
Enabling Privacy Protection remotely.....	<a href="#">71</a>
Selecting data to hide: Privacy Protection.....	<a href="#">73</a>
Creating a list of private numbers.....	<a href="#">74</a>

## PRIVACY PROTECTION

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

You can enable Privacy Protection from Kaspersky Mobile Security 9 or remotely from another mobile device. However, Privacy Protection can only be disabled from within the application.

## PRIVACY PROTECTION MODES

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

By default, Privacy Protection is disabled.

The following modes of Privacy Protection are available:

- **The Privacy Protection mode set to Normal** – hiding confidential information is disabled. The Privacy Protection settings are accessible for modification.
- **The Privacy Protection mode set to Private** – hiding confidential information is activated. The Privacy Protection settings cannot be changed.

You can set Privacy Protection to start automatically (see section "Enabling Privacy Protection automatically" on page [70](#)) or start remotely from another device (see section "Enabling Privacy Protection remotely" on page [71](#)).

The current mode of hiding confidential information is displayed in the application's main window in the **Privacy Protection** module

## ENABLING/DISABLING PRIVACY PROTECTION

➔ To change the Privacy Protection mode:

1. In the main window of Kaspersky Mobile Security 9, open the module **Privacy Protection**.
2. Click **Hide information** (see Figure below).

The name of the item changes depending on the Privacy Protection mode. If the **The Privacy Protection mode set to Normal** mode is set, the item is called **Hide information**. If **Confidential information is hidden** mode is set, the item is called **Show information**.

Changing the mode of Privacy Protection can take some time.

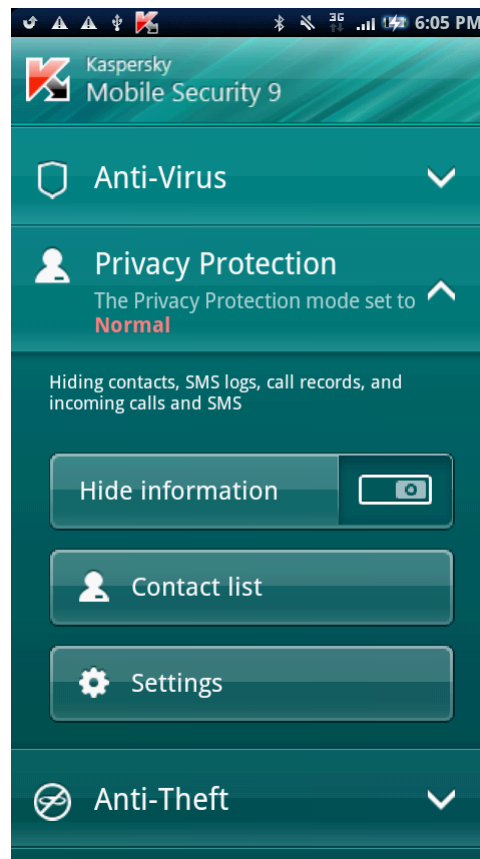


Figure 23. Changing Privacy Protection mode

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

The switch icon to the right of the item **Hide information** / **Show information** is changed depending on the mode selected.

## ENABLING PRIVACY PROTECTION AUTOMATICALLY

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

Disable Privacy Protection prior to editing Privacy Protection settings.

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

1. In the main window of Kaspersky Mobile Security 9, the **Privacy Protection** module is expanded.
2. Click **Settings**.

The **Privacy Protection Settings** window opens.

3. Select a value for the **Automatic hiding** setting depending on the following tasks (see Figure below):

- To disable the automatic activation of hiding confidential information, select **Disabled**.
- To start hide confidential information within a set period of time after the device switches to energy-saving mode, select one of the following values:
  - **No delay.**
  - **After 1 minute.**
  - **After 5 minutes.**
  - **After 15 minutes.**
  - **After 1 hour.**

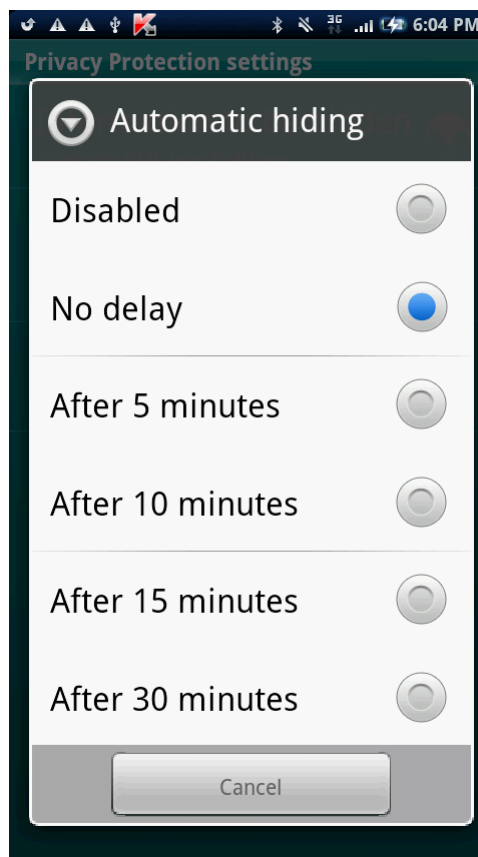


Figure 24. Automatic start of Privacy Protection

## ENABLING PRIVACY PROTECTION REMOTELY

Kaspersky Mobile Security 9 allows you to enable Privacy Protection remotely from another mobile device. To accomplish this, first activate the Hide on SMS command option on your device.

➔ To allow remote enabling of Privacy Protection:

1. In the main window of Kaspersky Mobile Security 9, open the module **Privacy Protection**.
2. Click **Settings**.  
The **Privacy Protection Settings** window opens.
3. Check the **Hide on SMS Command** box (see Figure below).

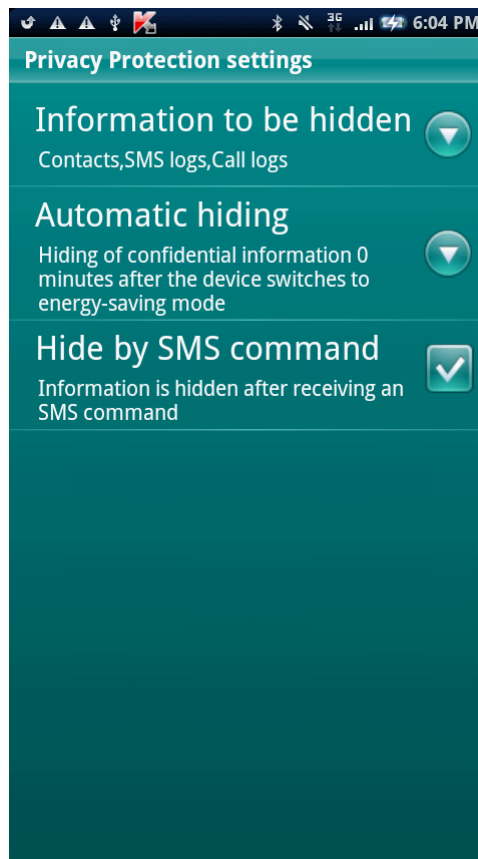


Figure 25. Privacy Protection remote enabling settings

You can enable Privacy Protection remotely 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. As a result, your device unnoticeably receives an SMS, and confidential information is hidden. To create a special SMS command, use the Sending a command function.
- On another mobile device, create and send an SMS message with a special text and the secret code of the application specified on your device. As a result, the device receives an SMS, and confidential information is hidden.

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

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

1. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.
2. This will open the **Additional** window.
3. Select **Send command**.
4. For the **SMS command** set the value **Privacy Protection**.
5. In the **Phone number receiving the SMS command** field, enter the telephone number of the device receiving the SMS command.
6. In the **Secret code of the device receiving the SMS command** field, enter the application's secret code stated on the device receiving the SMS command.
7. Press **Send**.

When an SMS command is received on the device, Kaspersky Mobile Security 9 activates the hiding of confidential information and information on the device is hidden.

➤ *To enable Privacy Protection remotely using a telephone's standard tools for creating an SMS:*

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

## SELECTING DATA TO HIDE: PRIVACY PROTECTION

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

Disable Privacy Protection prior to editing Privacy Protection settings.

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

1. In the main window of Kaspersky Mobile Security 9, open the **Privacy Protection** module.
2. Click **Settings**.

The **Privacy Protection Settings** window opens (see Figure below).

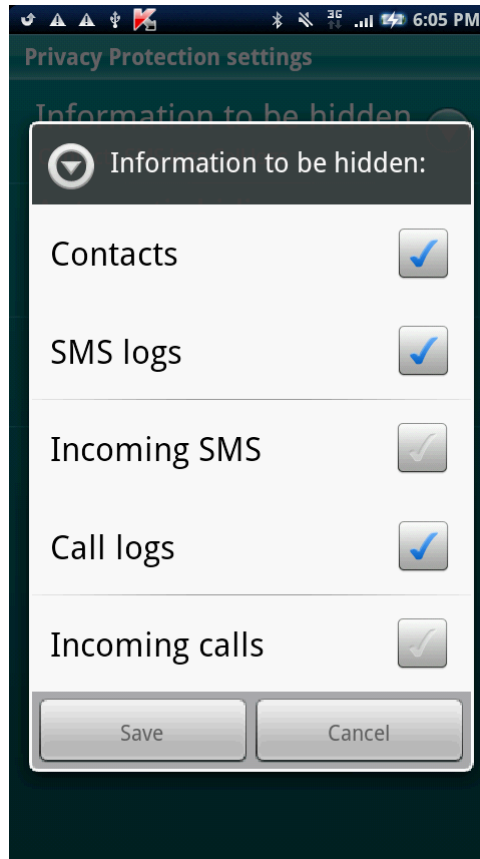


Figure 26. Selecting hidden information and events

3. Select information and events which are hidden for confidential numbers. To do this, set **Information to be hidden** and set the check box next to the settings required. The following settings are available:
  - **Contacts** – hide all information about confidential numbers in the Contacts.
  - **SMS logs** — hide SMS messages in the **Incoming**, **Outgoing** and **Sent** folders for confidential numbers.
  - **Incoming SMS** – hide incoming SMS from private numbers.
  - **Call logs** – accept calls from confidential numbers, but do not show the caller number and do not display information about confidential numbers on the list of calls (incoming, outgoing, and missed).
  - **Incoming calls** – block calls from private numbers (caller will hear the engaged tone in this case). Information about a received call will be displayed when Privacy Protection is disabled.

## CREATING A LIST OF PRIVATE NUMBERS

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

Before making the Contact List, disable hiding confidential information.

**IN THIS SECTION**

Adding a number to the list of private numbers .....	<a href="#">75</a>
Editing a number in the list of private numbers .....	<a href="#">76</a>
Deleting a number from the list of private numbers .....	<a href="#">77</a>

## ADDING A NUMBER TO THE LIST OF PRIVATE NUMBERS

You can add telephone numbers to the Contacts list manually or import them from Contacts.

Before making the Contact List, disable hiding confidential information.

➤ *To add a phone number to the Contact list:*

1. In the main window of Kaspersky Mobile Security 9, open the module **Privacy Protection**.

2. Click **Contact list**.

The **Contact list** window will open.

3. Perform one of the following actions (see Figure below):

- To add a number from Contacts, select **Add** → **Contacts**. Select the required entry from the Contact List in the window that opens.
- To add a number, select **Add** → **Number**, complete the **Phone number** field and press **Save**.

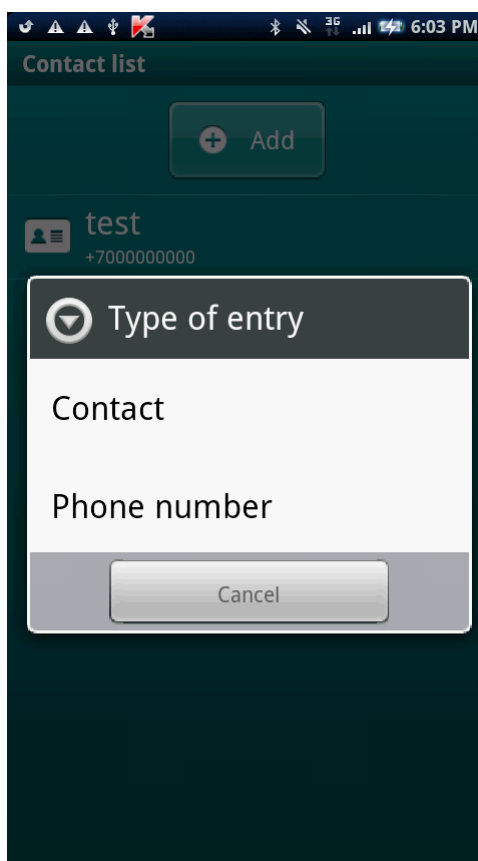


Figure 27. Adding entries to the list of protected contacts

The number will be added to the Contact list.

## EDITING A NUMBER IN THE LIST OF PRIVATE NUMBERS

Disable Privacy Protection prior to editing Privacy Protection settings.

Phone numbers added manually are only available for editing on the Contact List. It is not possible to edit numbers that have been selected from Contacts.

➤ *To edit a phone number on the Contact List:*

1. In the main window of Kaspersky Mobile Security 9, open the **Privacy Protection** module.
2. Click **Contact list**.

The **Contact list** window will open.

3. Select from the Contact list a number for editing and select **Edit** in the context menu.

The **Editing a number** window opens.

4. Change the data in the **Phone number** field.
5. When completing the editing, press **Save**.

The number is changed.

## DELETING A NUMBER FROM THE LIST OF PRIVATE NUMBERS

You can delete one number or clear the list of Contact List completely.

Disable Privacy Protection prior to editing Privacy Protection settings.

➤ *To remove a number from the Contact List:*

1. In the main window of Kaspersky Mobile Security 9, the **Privacy Protection** module is expanded.
2. Click **Contact list**.  
The **Contact list** window will open.
3. Select the number to be deleted and select **Delete** in the context menu.  
The confirmation window opens.
4. Confirm deletion. To do this, press **Yes**.

➤ *To clear the Contact List:*

1. In the main window of Kaspersky Mobile Security 9, open the **Privacy Protection** module.
2. Click **Contact list**.  
The **Contact list** window will open.
3. Select **Delete all** in the context menu.  
The confirmation window opens.
4. Confirm deletion. To do this, press **Yes**.

The Contact List becomes empty.

# UPDATING THE APPLICATION'S DATABASES

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

## IN THIS SECTION

About updating the application's databases .....	<a href="#">78</a>
Starting updates manually .....	<a href="#">79</a>
Starting scheduled updates .....	<a href="#">79</a>

## ABOUT UPDATING THE APPLICATION'S DATABASES

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

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

Kaspersky Mobile Security 9 performs application database updates from the Kaspersky Lab update servers. These are special Internet sites which contain updates for databases for all Kaspersky Lab products.

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

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

1. The application databases installed on your mobile device are compared with those located on the special Kaspersky Lab update server.
2. Kaspersky Mobile Security 9 performs one of the actions:
  - If you have the latest anti-virus databases installed, an information message is displayed on the screen.
  - If the installed anti-virus databases are different, a new update package is downloaded and installed.

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

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

When roaming, it is possible to disable Kaspersky Mobile Security 9 anti-virus database update in order to avoid unnecessary costs.

Detailed information on the antivirus databases used is accessible in the **Anti-Virus** → **Additional** module in the **Start update**.

## STARTING UPDATES MANUALLY

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

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

1. In the main window of Kaspersky Mobile Security 9, open the module **Anti-Virus** folder.
2. Click **Additional**.  
  
The **Anti-Virus: Additional** window opens.
3. Click **Start update**.

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

## STARTING SCHEDULED UPDATES

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

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

Additionally, you can set the automatic update when you are roaming.

➤ *To configure a scheduled update start:*

1. In the main window of Kaspersky Mobile Security 9, expand the **Antivirus** module.
2. Click **Additional**.  
  
The **Anti-Virus: Additional** window opens.
3. Select **Update settings**.  
  
The **Update settings** window opens
4. Set one of the following values for the **Scheduled update** settings:
  - **Weekly**: update application databases once a week. Select the values for the **Start day** and **Start time**.
  - **Daily**: update application databases every day. Enter the value for the **Update time**.
  - **Disabled** – do not update the application's databases on schedule.

# CONFIGURING ADDITIONAL SETTINGS

The section provides information on the additional options of Kaspersky Mobile Security 9: how to enable / disable emerging messages in the status line on the application's operation, audio notification, display of prompts before adjusting the settings of every component, how to set the home screen widget, and how to change the application's secret code.

## IN THIS SECTION

---

Changing the secret code .....	<a href="#">80</a>
Displaying prompts.....	<a href="#">80</a>
Configuring sound notifications .....	<a href="#">81</a>
Messages in the status line .....	<a href="#">81</a>

## 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. In the main window of Kaspersky Mobile Security 9 expand the **Additional** module.  
This will open the **Additional** window.
2. Select **Change secret code**.
3. Enter the current secret code of the application in the **Enter secret code** entry field.
4. Enter the application's new secret code in the **Set new secret code** field.

The code entered is automatically verified.

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

5. Enter this code again in the **Repeatedly enter the new code** field.

The secret code is changed.

## 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. In the main window of Kaspersky Mobile Security 9, open the module **Additional** tab.

This will open the **Additional** window.

2. Perform actions depending on the following tasks:
  - To enable the display of prompts, check the **Hints** checkbox.
  - To disable the display of prompts, remove the **Hints** checkbox.

## CONFIGURING SOUND NOTIFICATIONS

As a result of the application's operation, events arise, for instance, an infected file is detected, the license's term of validity has expired. For the application to inform you in every such event, you can enable sound notification of the occurring event.

Kaspersky Mobile Security 9 includes sound notification only according to the device's set mode.

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

1. In the main window of Kaspersky Mobile Security 9, open the module **Additional** tab.  
This will open the **Additional** window.
2. Perform actions depending on the following tasks:
  - To enable audio notification, check the **Sound** checkbox.
  - To disable audio notification, remove the **Sound** notification.

## MESSAGES IN THE STATUS LINE

Kaspersky Mobile Security 9 allows receiving of emerging notifications in the status line about application events, for example, on starting the application, on the expiry of the license's validity or on the disabling of protection. You can enable / disable the receiving of notifications on application events in the status line.

➤ *To manage emerging notifications on the application's operation, proceed as follows:*

1. In the main window of Kaspersky Mobile Security 9, open the module **Additional** tab.  
This will open the **Additional** window.
2. Perform actions depending on the following tasks:
  - To enable emerging notifications on the application's operation, check the **Notifications** checkbox.
  - To disable emerging notifications, remove the **Notifications** checkbox.

When using Kaspersky Mobile Security 9, the home screen widget is accessible (see page [33](#)). The home screen widget is intended for the indication of the protection status of your device, the hiding of confidential information and the application's license.

After installing the application, the widget automatically appears in the device's main window. You can add a widget to the main window or delete it and also set the indication of hiding confidential information in the Home screen widget (see section "Hiding confidential information" on page [69](#)).

➤ *To manage the display of the widget in the main window, proceed as follows:*

1. In the main window of Kaspersky Mobile Security 9, open the **Additional** tab.  
This will open the **Additional** window.

2. Select **Widget**.

The **Home screen widget** window opens.

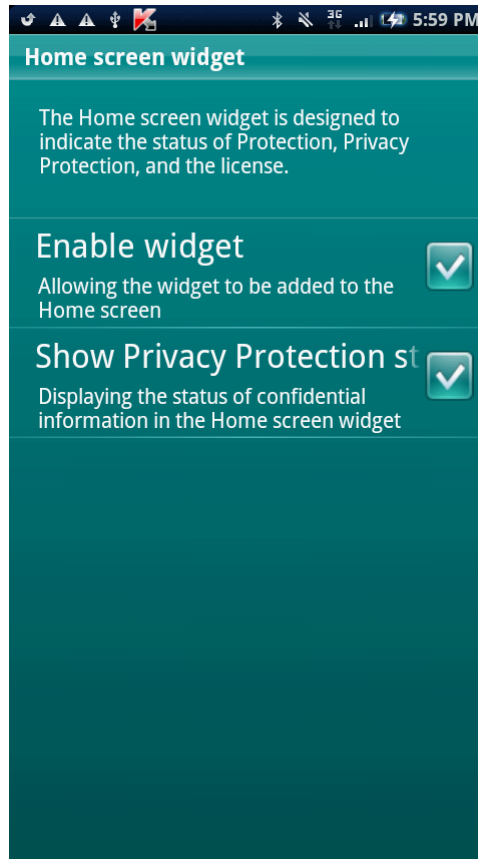


Figure 28. Home screen widget settings

3. Perform actions depending on the following tasks:

- To display a change to the mode of hiding confidential information in the Home screen widget, check the **Enable widget** checkbox.
- To delete the widget from the Home screen widget, uncheck the **Enable widget** checkbox.

➡ To set the indication of the status of confidential information in the Home screen widget, proceed as follows:

1. In the main window of Kaspersky Mobile Security 9, open the **Additional** module.

This will open the **Additional** window.

2. Select **Widget**.

The **Home screen widget** window opens.

3. Perform actions depending on the following tasks:

- To display a change to the mode of hiding confidential information in the Home screen widget, check the **Show Privacy Protection status** checkbox
- To hide a change to the mode of hiding confidential information in the Home screen widget, check the **Show Privacy Protection status** checkbox.

# CONTACTING THE TECHNICAL SUPPORT SERVICE

If you have already purchased Kaspersky Internet Security, you can obtain information about it from the Technical Support Service, either over the phone or via the Internet.

Technical Support Service specialists will answer any of your questions about installing and using the application. They will also help you to eliminate the consequences of malware activities if your device has been infected.

Before contacting the Technical support service, please read the Support rules for Kaspersky Lab's products (<http://support.kaspersky.com/support/rules>).

## E-mailing your question to the Technical Support Service

You can forward your question to the Technical Support Service specialists by filling out a Helpdesk web form at (<http://support.kaspersky.com/helpdesk.html>).

You can write your inquiry in Russian, English, German, French or Spanish.

To send an e-mail message with your question, you must include the **Customer ID** and **password** you received when you registered at the Technical Support Service's website.

If you are not a registered user of Kaspersky Lab's applications, you can fill out a registration form (<https://support.kaspersky.com/personalcabinet/registration/form/>). During registration enter the *activation code* for your application, or the *key filename*.

The Technical Support Service will respond to your request in your Personal Cabinet (<https://support.kaspersky.com/PersonalCabinet>) and to the e-mail address you specified in your inquiry.

In your inquiry, please describe the problem you have encountered. Specify the following in the mandatory fields:

- **Request type.** Select a topic which corresponds to the arising problem most closely, for instance "Product Installation/Removal Problem" or "Anti-Virus scan/virus removal problem". If you do not find an appropriate topic, select "General question".
- **Application name and version number.**
- **Request text.** Describe the problem you encountered, providing as much relevant detail as possible.
- **Customer ID and password.** Enter the customer ID and password you received when you registered at the Technical Support Service's website.
- **E-mail address.** The Technical Support Service will reply to your question at this email address.

## Technical support by phone

If you have an urgent problem, you can call your local Technical Support Service. Before contacting your local ([http://support.kaspersky.com/support/support\\_local](http://support.kaspersky.com/support/support_local)) or international (<http://support.kaspersky.com/support/international>) Technical Support Service, please collect the necessary information (<http://support.kaspersky.com/support/details>) about your device and the installed anti-virus application. This will enable our specialists to help you more quickly.

# GLOSSARY

## A

### ACTIVATING THE APPLICATION

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

### ANTI-VIRUS DATABASES

Databases created by Kaspersky Lab's experts and containing detailed description of all currently existing threats to computer security as well as methods used for their detection and disinfection. These databases are constantly updated by Kaspersky Lab as new threats appear.

### APPLICATION SECRET CODE

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

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

## ARCHIVE

File "containing" one or several other objects which can also be archives.

## 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.

### DELETION OF AN OBJECT

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

## DISINFECTING OBJECTS

A method used for processing infected objects, resulting in complete or partial recovery of data, or a decision that the objects cannot be disinfected. Disinfection of objects is performed based on the application database. Part of a file's legitimate data may be lost during the disinfection process.

## I

### INFECTED OBJECT

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

## 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 delivers 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](mailto: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 .....	<a href="#">87</a>
Other information .....	<a href="#">89</a>

## DISTRIBUTED PROGRAM CODE

The independent program code of external manufacturers is distributed along with the program in its original or binary form without making any changes.

## IN THIS SECTION

---

ADB.....	<a href="#">87</a>
ADBWINAPI.DLL .....	<a href="#">87</a>
ADBWINUSBAPI.DLL .....	<a href="#">87</a>

## 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.....	21
license .....	27
Activation	
Call&SMS Filter .....	45
Adding	
Call&SMS Filter Black List.....	47
Call&SMS Filter White List.....	50
list of confidential Privacy Protection numbers .....	75
Allowing	
incoming calls .....	50
incoming SMS .....	50
Anti-Theft.....	58
Block.....	59
Data Wipe.....	60
GPS Find.....	65
SIM Watch.....	63
Application secret code .....	24, 25
Archives	
On-demand scans .....	42

## B

Black List	
Call&SMS Filter .....	46
Blocking	
device .....	59
incoming calls .....	46
incoming SMS .....	46

## C

Call&SMS Filter.....	44
action in respect of a call .....	55
action in respect of SMS.....	54
Black List .....	46
modes.....	45
non-numerical numbers.....	53
numbers not from Contacts .....	52
White list.....	49
Code	
activation code.....	22, 23
application secret code .....	24

## D

Data	
remote delete.....	60
DATA	
CONFIDENTIAL INFORMATION .....	69
Delete	
Call&SMS Filter Black List.....	49
Call&SMS Filter White List.....	52
Deleting	
list of confidential Privacy Protection contacts .....	77
Determining the device's location.....	65
Disabling	

Call&SMS Filter .....	45
Privacy Protection.....	70
<b>E</b>	
Edit	
Call&SMS Filter Black List.....	48
Call&SMS Filter White List.....	51
Editing	
list of confidential Privacy Protection contacts .....	76
Enabling	
Privacy Protection.....	70
Entry	
Call&SMS Filter Black List.....	47
Call&SMS Filter White List.....	50
<b>F</b>	
FILTERING	
INCOMING CALLS.....	44
INCOMING SMS .....	44
<b>I</b>	
INSTALLING THE APPLICATION .....	19
<b>L</b>	
License	
activating the application .....	21
information.....	28
License Agreement.....	27
renewal.....	29
<b>M</b>	
Modes	
Call&SMS Filter .....	45
Privacy Protection.....	69, 70
<b>O</b>	
On-demand scans	
Actions to be performed on objects .....	42
archives .....	42
scheduled start .....	40
<b>P</b>	
Privacy Protection .....	69
automatic start.....	70
list of confidential contacts.....	74
modes.....	69
remote start .....	72
selecting information and events to be hidden.....	73
<b>R</b>	
Renewing the license .....	29
<b>S</b>	
Schedule	
On-demand scans .....	40
Update .....	79
Send SMS command .....	67
Sound.....	81

Starting application .....26

**U**

UNINSTALLING APPLICATION.....20

Updating scheduled start .....79

**W**

White list Call&SMS Filter .....49

Wipe information saved on the device .....60