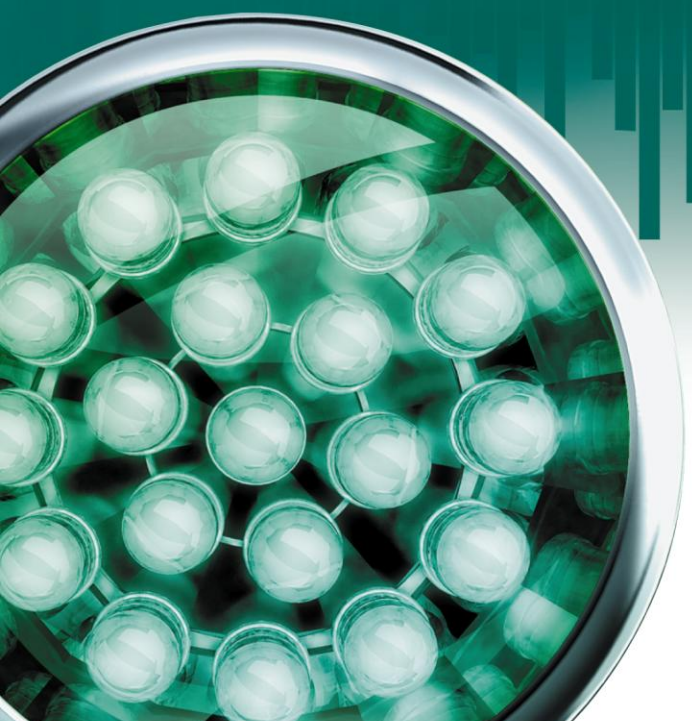
Kaspersky Mobile Security 9

for Symbian OS

USER GUIDE

PROGRAM VERSION: 9.0



KASPERSKY lab

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.

Revision date: 20.01.2011

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, INFORMATON, 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 LIABILE, 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 EXLUDED 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 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, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

TABLE OF CONTENTS

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

The following sections are included in the document:

Additional data sources

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

Kaspersky Mobile Security 9

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

Installing Kaspersky Mobile Security 9

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

Uninstalling the application

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

Updating the application

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

Getting started

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

Managing the license

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

Application interface

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

File system protection

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

Scanning the device

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

Quarantining malware objects

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

Filtering of incoming calls and SMS

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

Restricting outgoing calls and SMS messages. Parental Control

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

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

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

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

Privacy Protection

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

Filtering network activity. Firewall

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

Encrypting personal data

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

Updating the application's databases

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

Application logs

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

Configuring additional settings

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

Contacting the Technical Support Service

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

Glossary

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

Kaspersky Lab

The section provides information on Kaspersky Lab ZAO.

Information about third party code

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

Index

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

DOCUMENT CONVENTIONS

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

Table 1. Document conventions

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

ADDITIONAL DATA SOURCES

If you have questions about setting up or using Kaspersky 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

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

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.

To open the context help, open the required screen and select **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.

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. 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 Symbian OS operating system. The application can protect information on the device from infection by known threats, prevent unwanted SMS messages and calls, control the network connection on the device, encrypt information, hide it for confidential contacts and also protect information if the device is lost or stolen. 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**. This protects information on the device from unauthorized access when it is lost or stolen and also makes it easier to find. Anti-Theft enables you to lock your device remotely, delete any information stored there, and pinpoint its geographic location (if your mobile device has a GPS receiver) using SMS commands from another device. Furthermore, Anti-Theft allows you to lock your device if the SIM card is replaced or if the device is activated without a SIM card.

- **Parental Control**. All outgoing SMS messages and calls are checked. The component allows flexible configuration of the filtering of outgoing SMS and calls.

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

- **Firewall**. Checks the network connections on your mobile device. Firewall sets the connections which will be permitted or prohibited.

- **Encryption**. This protects information in encrypted mode. The component encrypts any amount of non-system folders which are in the device memory or on storage cards. Access to files from encrypted folders is only possible after entering the secret application code.

Furthermore, the application contains a series of service functions which allow maintaining the application in up-to-date condition, expanding the application's options of use and supporting the user in his operations:

- Protection status. The status of the program's components is displayed on screen. Based on the information presented, you can evaluate the current information protection status on your device.

- Update the application's anti-virus databases. This function keeps Kaspersky Mobile Security 9 anti-virus databases up to date.

- Events log. The application for each component has its own Events log with information on the operation of the component (e.g. scan report, update of anti-virus databases, information about blocked files). Reports on the operation of components are given in the remote administration system and remain in it.

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

IN THIS SECTION

WHAT'S NEW IN KASPERSKY MOBILE SECURITY 9

Below is a detailed view of the novelties with Kaspersky Mobile Security 9.

Kaspersky Mobile Security 9 includes the following new options:

- Access to the application is protected by a secret code.
- The Privacy Protection component allows you to hide the following information for confidential contacts from the Contact list: entries in Contacts, SMS messages, call log, and new incoming SMS messages and incoming calls. Confidential information is accessible for viewing for hiding is disabled.
- Encryption allows the encryption of folders saved in the device memory or on a memory card. The component protects confidential data in encrypted mode and allows access to encrypted information only when the application secret code is entered.
- A new service function has been added, called Show hints: Kaspersky Mobile Security 9 for Smartphone shows a short description of a component before configuration of its settings.
- You can buy an activation code or extend your license validity period either directly from your mobile device through the subscription option or online.

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.

HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Mobile Security 9 can be installed on mobile devices working on Symbian OS 9.1, 9.2, 9.3 and 9.4 Series 60 UI.

INSTALLING KASPERSKY MOBILE SECURITY 9

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

To install Kaspersky Mobile Security 9:

1. Connect the mobile device to the computer.

   For Nokia mobile devices, it is recommended to use the Nokia PC Suite or Nokia Ovi Suite application.

2. Perform one of the following actions:

   - If you have purchased the program on a CD, run the automatic Kaspersky Mobile Security 9 installation on the CD purchased.
   - If you have purchased the distribution package on the Internet, copy it to the mobile device, using one of these methods:
     - from the Nokia PC Suite or Nokia Ovi Suite application (for Nokia mobile devices);
     - using a memory card.

     Start the installation using one of the following methods:

     - from the Nokia PC Suite or Nokia Ovi Suite application (for Nokia mobile devices);
     - open the SIS archive containing the distribution package on your mobile device.

   A window confirming the installation opens.

3. Confirm the installing of the application by pressing the **Yes** button.

4. Review the additional information about the application, which includes name, version, and certificates. Then press **Continue**.

   If the language of the operating system does not match the language of Kaspersky Mobile Security 9, a message is displayed on the screen. To proceed with the installation in the current language, press **OK**.

5. Read the License Agreement text, which is concluded between you and Kaspersky Lab. If you agree to all terms of the agreement, press **OK**. The installation of Kaspersky Mobile Security 9 will then start. If you do not agree to the terms of the License Agreement, press **Cancel**. Installation will be terminated.

6. Confirm that there are no other anti-virus applications on the device by pressing **OK**.

7. In order to complete the installation, restart the device.

   The application is installed with the parameters recommended by the experts of Kaspersky Lab.

UNINSTALLING THE APPLICATION

To uninstall Kaspersky Mobile Security 9:

1. Decrypt the data on your device if it was encrypted with Kaspersky Mobile Security 9 (see the "Data decryption" section on page 104).

2. Disable Privacy Protection (see section "Privacy Protection modes" on page 92).

3. Close Kaspersky Mobile Security 9. To do this, select **Options** → **Exit** (see Figure below).

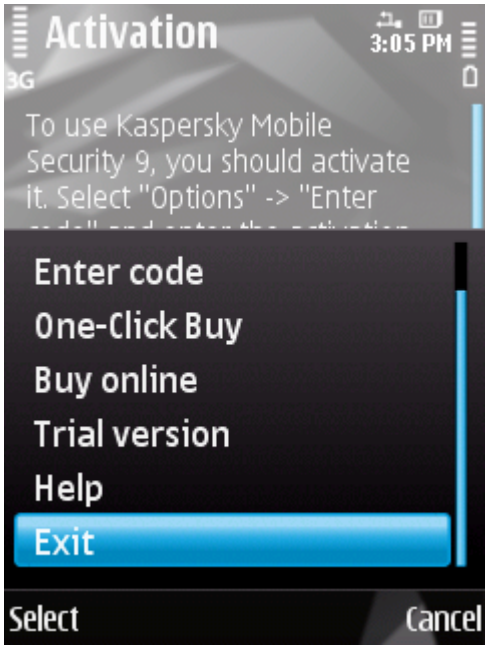


Figure 1: Exiting the application

4. Uninstall Kaspersky Mobile Security 9. To do this, perform the following actions:

   a. Open the device's main menu.

   b. Select the **Applications** → **Applications** (see Figure below).

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

Figure 2: Path to installed applications

c. Select **KMS 9.0** from the list of applications and then select **Options** → **Remove** (see figure below).

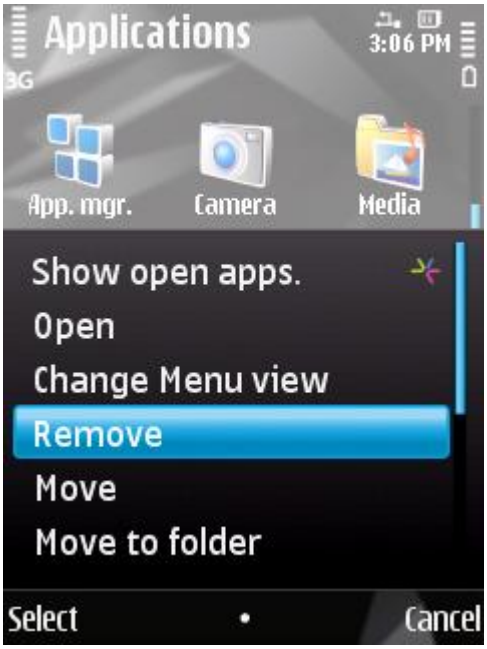


Figure 3: Uninstalling the application

d. Confirm the uninstalling of the application by pressing the **Yes** button.

e. Enter the secret code and press **OK**.

f. Specify whether or not to keep the application settings and objects in Quarantine:

- If you wish to save the application's parameters and objects to the quarantine, check the boxes opposite the parameters required and then press **OK** (see Figure below).

- In order to uninstall the application completely, press **Cancel**.

Figure 4: The list of settings to be saved

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

UPDATING THE APPLICATION

You can update Kaspersky Mobile Security 9 by installing the most recent version of the application in this generation (for example, update the version 9.0 for the version 9.2).

If you use Kaspersky Mobile Security 8.0, you can switch to Kaspersky Mobile Security 9.

To update the program version:

1. Decrypt the data on your device if it was encrypted with Kaspersky Mobile Security 9 (see the "Data decryption" section on page 104).
2. Disable Privacy Protection (see section "Privacy Protection modes" on page 92).
3. Close the current version of Kaspersky Mobile Security 9. To do this, press **Options** → **Exit**.
4. Copy the application's distribution package to your device, using one of these methods:
   - from the Kaspersky Lab website;
   - from the Nokia PC Suite or Nokia Ovi Suite application (for Nokia mobile devices);
   - using a memory card.
5. Start the Kaspersky Mobile Security 9 distribution package on the device.
6. Confirm the installing of the application by pressing the **Yes** button.
7. Review the additional information about the application, which includes name, version, and certificates. Then press **Continue**.
8. Confirm the update of the application version by pressing **OK**.
9. Enter the secret code set in the previous version of the application.
10. Read the license agreement carefully. If you agree to its terms, press **OK**. If you do not agree to the terms of the License Agreement, press **Cancel**. Installation will be terminated.
11. Confirm that there are no other anti-virus applications on the device. To do this, press **OK**.
12. Specify whether or not to keep the application settings and objects in Quarantine:
    - If you want to keep the application settings and objects in Quarantine, check the boxes for the required settings and press **OK**.
    - In order to uninstall the application completely, press **Cancel**.

    The installation of Kaspersky Mobile Security 9 starts.
13. In order to complete the installation, restart the device.

    If the current license is still valid, the application will be activated automatically. If the license has expired, activate the application (see section "Activating the application" on page 26).

To switch from Kaspersky Mobile Security 8.0 to the version 9:

1. Decrypt all data if they have been encrypted using Kaspersky Mobile Security 8.0.
2. Close Kaspersky Mobile Security 8.0. To do this, press **Options** → **Exit**.

3. Uninstall Kaspersky Mobile Security 8.0. To do this, perform the following actions:

   a. Open the device's main menu.

   b. Select the **Applications** → **My own** folder.

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

   c. Select **KMS 8.0** from the list of applications and select **Options** → **Remove**.

   d. Confirm the uninstalling of the application by pressing the **Yes** button.

   e. Delete the settings of Kaspersky Mobile Security 8.0 completely since they are incompatible with those of the version 9. To do this, press **Cancel**.

4. Restart the device to complete the uninstallation of Kaspersky Mobile Security 8.0.

5. Start installing Kaspersky Mobile Security 9 (see section "Installing Kaspersky Mobile Security 9" on page 20).

   If the validity period of the Kaspersky Mobile Security 8.0 license has not expired, enable program version 9 using the activation code of version 8.0 (see the "Activating the application" section on page 26).

GETTING STARTED

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

IN THIS SECTION

ACTIVATING THE APPLICATION

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

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

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

You can activate the application as follows:

- **Activate trial license**. When you activate the trial version, the application receives a free trial license. The validity period of the trial license is displayed on the screen after the activation is complete. Once the validity period of the trial license expires, the application's functions will be limited. The following features will only be available:
  - Activating the application;
  - managing the application license;
  - Kaspersky Mobile Security 9 Help system;
  - disabling Encryption;
  - 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

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

1. Open the device's main menu.
2. Select the **Applications** → **KMS 9.0**.

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

3. Start the application. To do this, press **Options** → **Open**.

   The Kaspersky Mobile Security 9 window opens.

4. Select **Options** → **Enter code**.

   The Kaspersky Mobile Security 9 activation window opens.

5. Enter the code into the four fields. The activation code consists of Latin alphabet characters and digits. The code is case-insensitive. After entering the activation code, select **Options** → **Activate** (see Figure below).

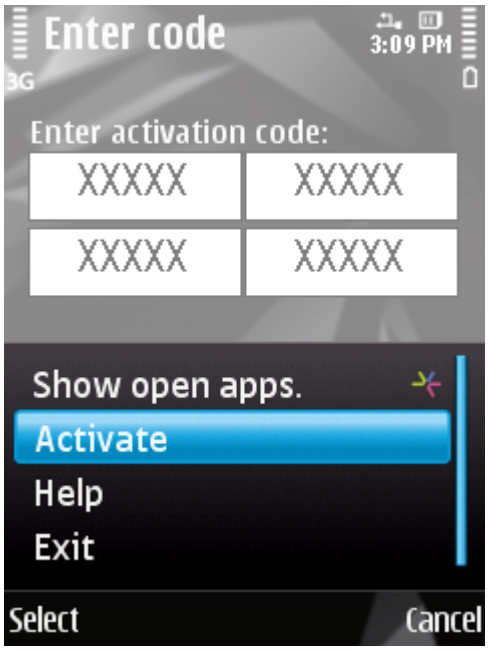


Figure 5: Activating a commercial version of the application

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

7. Select the access point via which the Kaspersky Lab activation server will be connected to.

   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.

8. Go to setting the secret code (see the "Setting the secret code" section on page 31).

ACTIVATING THE SUBSCRIPTION FOR KASPERSKY MOBILE SECURITY 9

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

To activate the subscription for Kaspersky Mobile Security 9:

1. Open the device's main menu.

2. Select the **Applications** → **KMS 9.0**.

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

3. Start the application. To do this, press **Options** → **Open**.

   The Kaspersky Mobile Security 9 window opens.

4. Select **Options** → **One-Click Buy** (see Figure below).

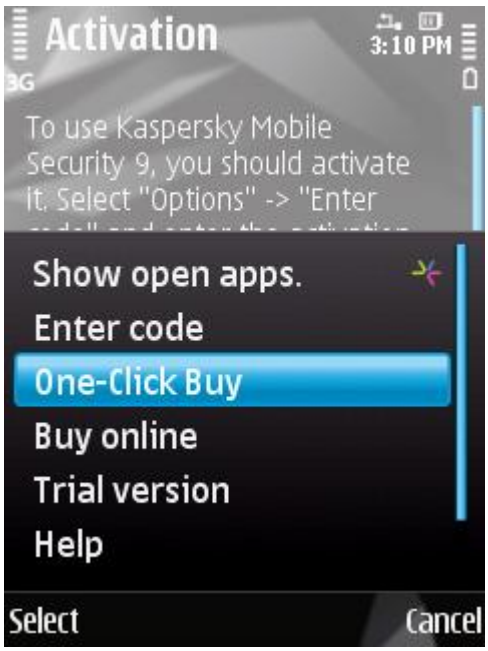


Figure 6: Activation of subscription

   The Kaspersky Mobile Security 9 activation window opens.

5. Confirm the activation of the subscription for Kaspersky Mobile Security 9 by pressing **Yes**.

6. Select the access point via which the application should connect to the activation server of Kaspersky Lab, and press **Yes**.

   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.

7. Read through the terms of subscription and, if you agree them, press **Yes**.

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

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

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

   If you do not agree the terms of subscription, click **No**. 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.

8. Go to entering the secret code (see the "Setting the secret code" section on page 31).

PURCHASING AN ACTIVATION CODE ONLINE

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

1. Open the device's main menu.
2. Select the **Applications** → → **KMS 9.0**.

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

3. Start the application. To do this, press **Options** → **Open**.

   The Kaspersky Mobile Security 9 window opens.

4. Select **Options** → **Buy online**.

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

5. Press **Open** (see Figure below).

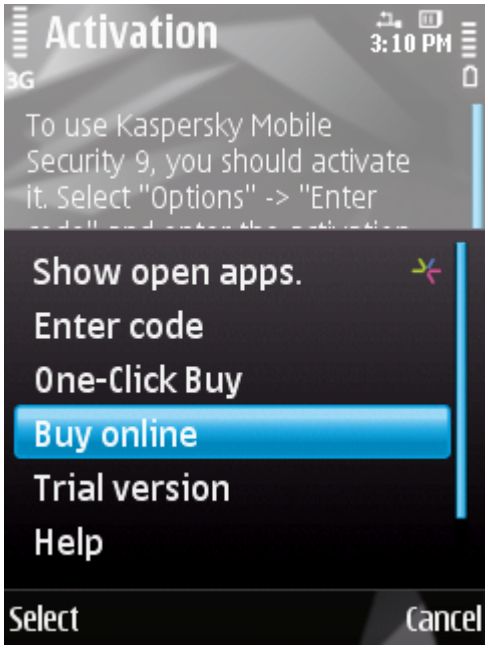


Figure 7: Purchasing the activation code online

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

6. Follow the step-by-step instructions.
7. After you are done with purchasing an activation code, proceed with activation of the commercial version of the application (see section "Activating the commercial version" on page 27).

ACTIVATING THE TRIAL VERSION

To activate the trial version of Kaspersky Mobile Security 9:

1. Open the device's main menu.

2. Select the **Applications** → **KMS 9.0**.

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

3. Start the application. To do this, press **Options** → **Open**.

   The Kaspersky Mobile Security 9 window opens.

4. Select **Options** → **Trial version** (see Figure below).

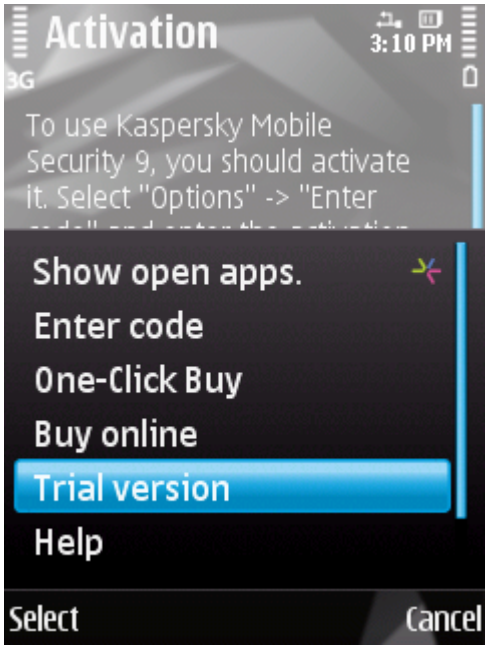


Figure 8: Trial license activation

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

6. Select the access point via which the server will be connected to and then press **OK**.

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

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

7. Go to entering the secret code (see the "Setting the secret code" section on page 31).

SETTING THE SECRET CODE

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

You can later change the secret code installed.

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

- for access to the application;
- for access to encrypted folders;

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

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 32). For this purpose, the recovery of secret code option must be enabled in advance (see the "Enabling the option to recover the secret code" section on page 32).

To enter the secret code:

1. After activating the application, enter in the **Enter new code** entry field, the digits of your new 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**.

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

3. Press **OK**.

   The secret code is now set.

ENABLING THE OPTION TO RECOVER THE SECRET CODE

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

If you have canceled the option enabling during the initial activation of the application, you can enable it after reinstallation of Kaspersky Mobile Security 9 on the device.

You can only recover the application secret code (see the "Recovering the secret code" section on page 32) if the recovery of secret code option is enabled. If you forget the password, and the recovery of secret code option is disabled, it will not be possible to manage the functions of Kaspersky Mobile Security 9, access encrypted files, or uninstall the application.

To enable the recovery of secret code option:

1. After you have installed the secret code for the application, confirm the enabling of the option of secret code recovery, by clicking **Yes**.

2. Enter your email address in the **Your email address** field and press **OK**.

   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 32).

To recover the application secret code:

1. Open the device's main menu.
2. Select the **Applications** → **KMS 9.0**.

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

3. Start the application. To do this, press **Options** → **Open**.

   The Kaspersky Mobile Security 9 window opens.

4. Press **Cancel**.

   A message will appear on the screen prompting you to go to recovery of the secret code.

5. Go to recovery of the secret code by pressing **Yes**.

   The following information will then be displayed on the screen:

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

6. Go to the website http://mobile.kaspersky.com/recover-code to recover your secret code.
7. 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.

8. On the application screen, press **Yes** and enter the recovery code that you have received.
9. Enter the new application secret code. To do this, enter a new application secret code in the field **Enter new code** and **Confirm code**.
10. Press **OK**.

STARTING THE APPLICATION

To start Kaspersky Mobile Security 9:

1. Open the device's main menu.
2. Select the **Applications** → **KMS 9.0**.

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

3. Start the application. To do this, press **Options** → **Open**.

   The Kaspersky Mobile Security 9 window opens.

4. Enter the secret code and press **OK**.

The application displays a window showing the current status of Kaspersky Mobile Security 9 (see the “Protection status window section” on page 43). To go to the application's functions, press **OK**.

UPDATING THE APPLICATION'S DATABASES

Kaspersky Mobile Security 9 scans for threats based on the application databases, which contain descriptions of all malicious programs known to date, methods for neutralizing them, and descriptions of other unwanted objects. At the time of installation, the anti-virus databases included in the Kaspersky Mobile Security 9 installation package may be out of date.

We recommend you to update the application's anti-virus databases immediately after the application installation.

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

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

  1. Select the **Update** item on the **Anti-Virus** tab.

     This will open the **Update** window.

  2. Select the **Update** item.

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

SCANNING THE DEVICE FOR VIRUSES

After installing the application, it is recommended to immediately run a scan of your mobile device for malware objects.

The first scan is performed with the settings previously set by the Kaspersky Lab experts.

- *To run a full scan of the device:*

  1. Select the **Scan** item on the **Anti-Virus** tab.

     This will open the **Scan** window.

  2. Select **Full scan**.

VIEWING INFORMATION ABOUT THE APPLICATION

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

- *To view information on the application,*

  On the **Additional** tab, 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

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 9.

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 35).

ABOUT KASPERSKY MOBILE SECURITY 9 LICENSES

A *license* is the right to use Kaspersky Mobile Security 9 and the additional services (see the "About the License Agreement" section on page 35) 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 (see section "Activating the commercial version" on page 27).

- *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, number of days until expiry, activation date, and device serial number.

To view the license information:

1. On the **Additional** tab, select **License**.

   This will open the **License** window.

2. Select the **About license** item (see Figure below).

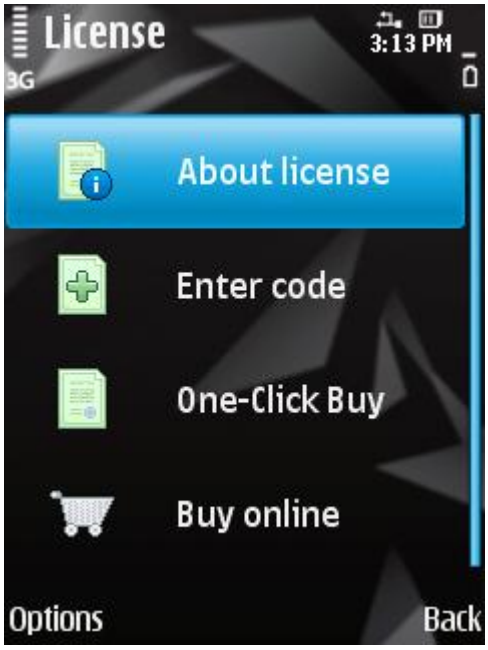


Figure 9: Viewing license information

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

RENEWING THE LICENSE

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

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

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

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

IN THIS SECTION

RENEWING THE LICENSE WITH THE ACTIVATION CODE

To renew the license with the activation code:

1. On the **Additional** tab, select **License**.

   This will open the **License** window.

2. Select **Enter code**.

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

3. Subsequently, enter the activation code obtained in four fields and then select **Options** → **Activate** (see Figure below).

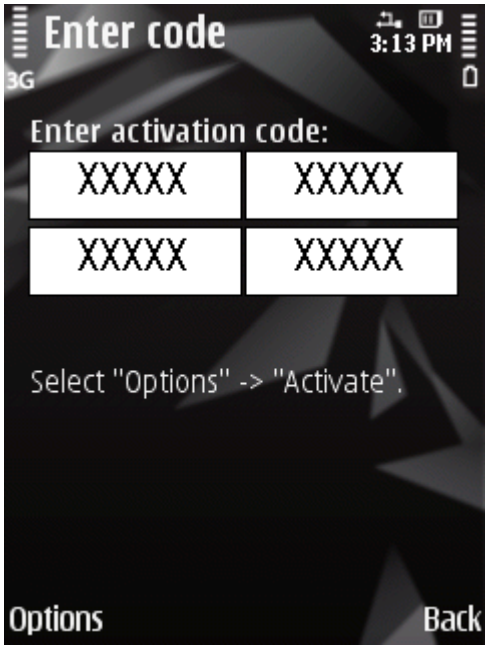


Figure 10: Renewing the license with the activation code

4. If the application additionally requests an application point, select the connection type required from the list of suggestions.

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

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

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

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

RENEWING THE LICENSE ONLINE

To renew your license online:

1. On the **Additional** tab, select **License**.

   This will open the **License** window.

2. Select **Renew online** (see Figure below).

Figure 11: Renewing the license online

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

3. Press **Open**.

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

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

4. Follow the step-by-step instructions.

5. When the order to renew the license is processed, enter the activation code obtained (see the "License renewal with activation code" section on page 38).

RENEWING THE LICENSE BY ACTIVATING THE SUBSCRIPTION

You can activate the subscription (see section "About Kaspersky Mobile Security 9 licenses" on page 35) for Kaspersky Mobile Security 9. When the subscription is activated, Kaspersky Mobile Security 9 renews the license each 30 days. Every time the license is renewed, the fixed amount specified in the terms of subscription is debited from your personal account.

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

To activate the subscription for Kaspersky Mobile Security 9:

1. Select the **Additional** tab, select **License**.

   This will open the **License** window.

2. Select the **One-Click Buy** tab (see figure below).

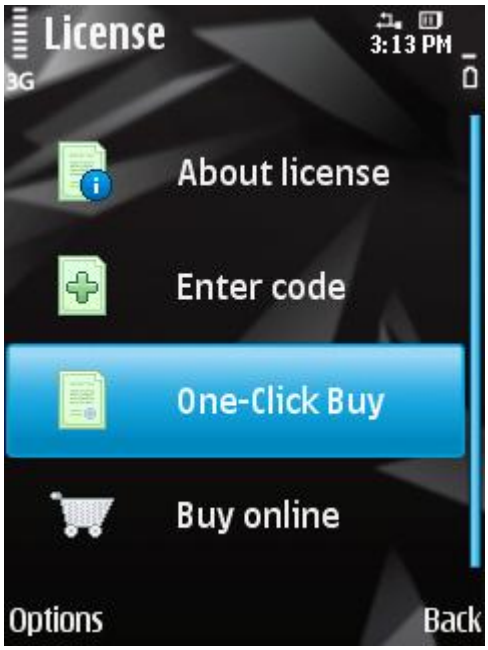


Figure 12: Activation of subscription

   This will open the **Activation** window.

3. Confirm the activation of the subscription for Kaspersky Mobile Security 9 by pressing **Yes**.

4. Select the access point via which the application should connect to the activation server of Kaspersky Lab, and press **Yes**.

   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.

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

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

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

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

   If you do not agree the terms of subscription, click **No**. In this case, the application will cancel the subscription activation and switch back to the screen on which you can select another method of renewing the license.

6. On completion, press **OK**.

UNSUBSCRIBING

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

If the subscription is canceled, you can resume it (see section "Resuming the subscription" on page 41).

To unsubscribe for Kaspersky Mobile Security 9:

1. On the **Additional** tab, select **License**.

   This will open the **License** window.

2. Select **Unsubscribe** (see Figure below).

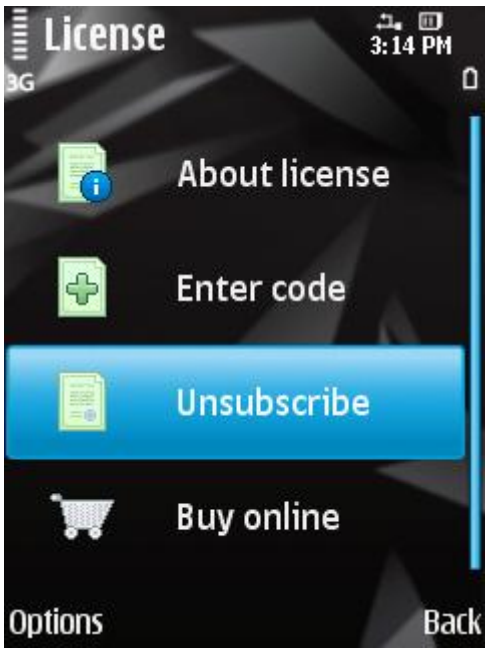


Figure 13: Unsubscribing

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

RENEWING THE SUBSCRIPTION

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

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

To resume the subscription:

1. Select the **Additional** tab, select **License**.

   This will open the **License** window.

2. Select the **One-Click Buy** tab.

If the current license has expired, Kaspersky Mobile Security 9 offers you to re-activate the subscription.

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 ICON

The protection icon displays the status of the application. If the icon is active (colored), this means that protection is switched on. If the icon is not active (gray), this indicates that the protection has been stopped and all its components are switched off.

By default, the protection icon is not displayed on the device's screen. You can edit the icon display settings (see section "Displaying the protection icon" on page 117).

SEE ALSO

PROTECTION STATUS WINDOW

The status of the application's main components is displayed in the current status window.

There are three possible statuses for every component, each is displayed with a color similar to the code of traffic lights. The green light means that the protection of your device is provided at the necessary level. Yellow and red indicate various types of threats. Threats do not only include outdated anti-virus application databases, but also, for instance, disabled protection components or minimum application operation settings.

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

- **Protection** is the protection status in real-time mode (see the "File system protection" section on page 47).

  The green status icon displays that protection is active and set at the correct level, and that the application's anti-virus databases are up to date.

  The yellow icon indicates that the anti-virus databases have not been updated for several days.

  The red icon color indicates problems which could result in a loss of information or infection of the device. For instance, protection is switched off. Perhaps the application anti-virus databases have not been updated for more than 15 days.

- **Firewall** is the level of protection of the device from unwanted network activity (see the "Filtering network activity. Firewall" section on page 100).

The green status icon shows that the component is active. Protection level of the Firewall is selected.

The red icon color indicates that network activity is not being filtered.

- **Anti-Theft** – status of data protection in case the device is lost or stolen (see the "Data protection in the event of loss or theft of the device" section on page 81).

  The green status icon means that the Anti-Theft function is active; its name is displayed under the component's status.

  The red colored icon shows that all Anti-Theft functions are disabled.

- **Privacy Protection** – is the status of hiding confidential information (see the "Privacy Protection" section on page 92).

  The green status icon shows that the component is active. Confidential data hidden.

  The yellow colored icon warns that the component is disabled. Personal data are displayed and accessible for viewing.

- **License** is the license's validity period (see the "Managing the license" section on page 35).

  The green status icon means that the license's validity period ends within more than 14 days.

  The yellow status icon means that the license's validity period ends within less than 14 days.

  The red icon indicates that your license has expired.

Figure 14: Current status window

You can also go to the status window by selecting **Options** → **Protection status**.

By default, the status window displays immediately after starting the application. You can change the settings of its display (see the "Status window display" section on page 116).

SEE ALSO

Displaying the status window 116

APPLICATION TABS

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

The Kaspersky Mobile Security 9 menu contains the following tabs:

- **Anti-Virus** - file system protection, on-demand scan and updating the application's anti-virus databases.
- **Privacy Protection** – hiding confidential information on the device.
- **Anti-Theft -** blocking the device and erasing information from it, if it is lost or stolen.
- **Encryption** – encryption of data on the device.
- **Call&SMS Filter** – filtering of unwanted incoming calls and SMS.
- **Parental Control** - control of outgoing calls and SMS.
- **Firewall** – control of network activity.
- **Additional** - general application settings, information about the application, databases in use and license.

By default, the application tabs are accessible after viewing the status window (see the "Protection status window" section on page 43).

It can be placed between the tabs as follows:

- using the device's joystick or stylus;
- selecting **Options** → **Open tab**.

APPLICATION MENU

The application menu allows fulfillment of the main tasks. The menu contains the following items (see Figure below):

- **Select**: selecting options, commands or settings.
- **Open tab**: takes you to the selecting of an application component.
- **Protection status**: takes you to the current Protection status window.
- **Help**: calls up the Kaspersky Mobile Security 9 context help.
- **About**: opens a window with details on the program.

- **Exit**: ends Kaspersky Mobile Security 9.

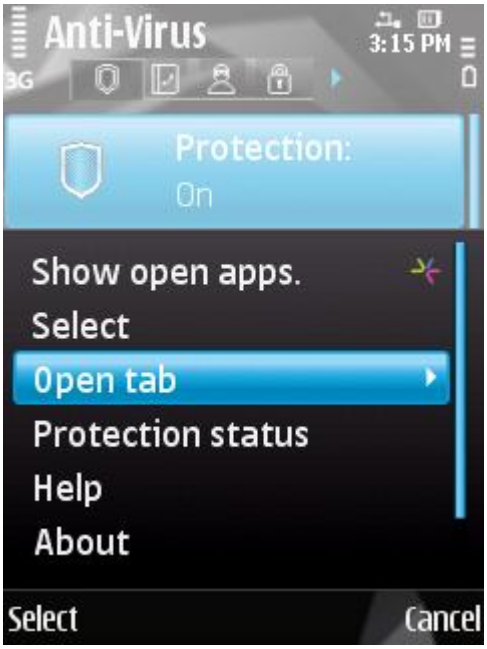


Figure 15: Application menu

In order to open the application menu,

select **Options**.

To navigate through the application menu, use the device's joystick or stylus.

FILE SYSTEM PROTECTION

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

IN THIS SECTION

ABOUT PROTECTION

Protection starts when operation system starts up and is always found in the device's memory. Protection scans all files that are opened, saved or run. 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 was detected in the file, the Protection blocks access to the file and performs the action specified in the settings;
    - If no malicious code is discovered in the file, it will be immediately restored.

Information on results from the operation of Protection is saved in the application's log (see the "Application logs" section on page 112).

ACTIVATE/DEACTIVATE PROTECTION

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

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

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

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

The current Protection status is displayed on the **Anti-Virus** tab next to the **Protection** menu item.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

- *To enable Protection:*

  1. Select the **Protection** item in the **Anti-Virus** tab.

     This will open the **Protection** window.

  2. For the **Protection mode** setting, select **On** (see figure below).

Figure 16: Enabling Protection

  3. Press **Back** to save the changes.

- *To disable Protection:*

  1. Select the **Protection** item in the **Anti-Virus** tab.

     This will open the **Protection** window.

  2. Select for the **Protection mode** setting the **Off** value.

  3. Press **Back** to save the changes.

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.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

- *To select the type of objects to be scanned:*

  1. Select the **Protection** item in the **Anti-Virus** tab.

This will open the **Protection** window.

2. Select a value for the **Objects to be scanned** setting (see Figure below):

   - **All files** - scan all types of files.
   - **Executables** – scan only executable application files (for instance, files of the formats EXE, SIS, MDL, APP).

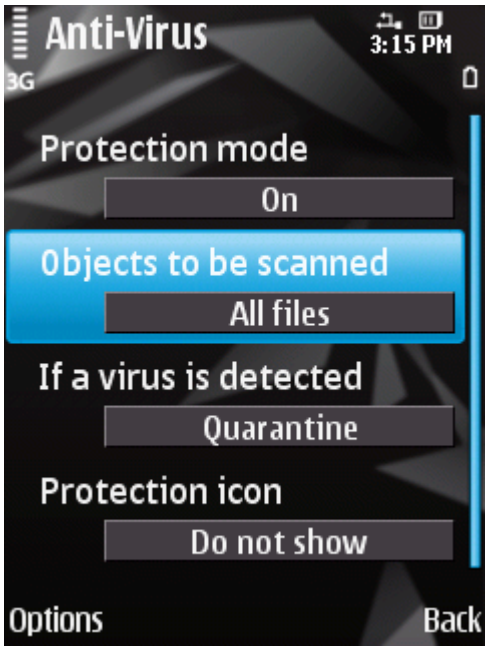


Figure 17: Selecting protection objects

3. Press **OK** to save the changes.

SELECTING THE ACTION TO BE PERFORMED ON DETECTED OBJECTS

Kaspersky Mobile Security 9 places by default the malicious objects found in the quarantine. You can choose the action that Kaspersky Mobile Security 9 performs when it detects a malicious object.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To configure the program's response when it detects a malware object:

1. Select the **Protection** item in the **Anti-Virus** tab.

   This will open the **Protection** window.

2. Set an action which the application takes if it finds a malicious object. To do this, select a value for the **If a virus is detected** setting (see Figure below):

   - **Delete**: delete malware objects without notifying the user.
   - **Quarantine**: quarantine malware objects.

- **Log event**: 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 18: The application's response to a malicious object

3. Press **OK** to save the changes.

RESTORING DEFAULT PROTECTION SETTINGS

Initially, the application contains the settings recommended by Kaspersky Lab experts. When setting Protection, you can always return to its recommended operation parameters.

To restore the default protection settings:

1. Select the **Protection** item in the **Anti-Virus** tab.

   This will open the **Protection** window.

2. Select **Options** → **Restore**.

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

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 files defined in the scan settings (see the "Selection of object type to be scanned" section on page 54).

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.

   After the analysis, Kaspersky Mobile Security 9 may take the following courses of action:

   - If malicious code was detected in the file, Kaspersky Mobile Security 9 blocks access to the file, and performs the action specified in the settings (see the "Selecting actions to be performed on objects" section on page 56).

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

The scan starts manually or automatically in accordance with a schedule (see the "Starting a scheduled scan" section on page 53).

Information about the on-demand scan's results is saved in the application's log (see the "Application logs" section on page 112).

STARTING A SCAN MANUALLY

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

To start an anti-virus scan manually:

1. Select **Scan** in the **Anti-Virus** tab.

   This will open the **Scan** window.

2. 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 the **Folder scan** item is selected, a window opens displaying the device's file system. To browse the file system, use the device's stylus or joystick buttons. In order to start the folder scan, select the required folder and select **Options** →**Scan**.

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

   - **Messages scan**: scan messages received by SMS, MMS or Bluetooth.

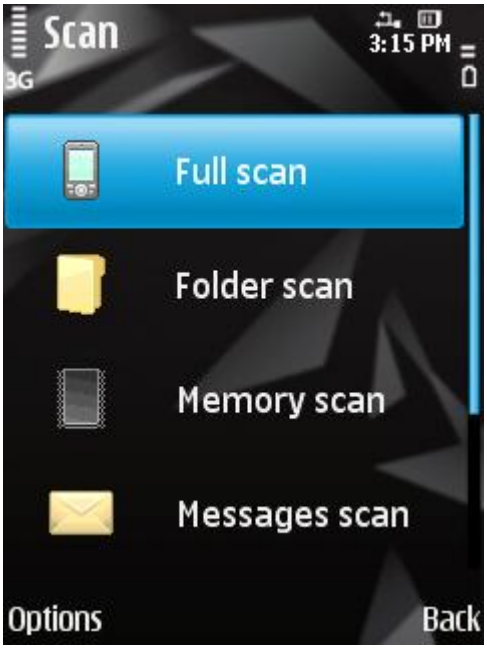


Figure 19: Selecting of scan area

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 (see figure below).

Figure 20: Device scan status

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 56).

By default, if the application detects a threat, it attempts to eliminate it. If this is not possible, the program places the infected object in quarantine.

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

- number of objects scanned;
- number of viruses detected, placed in the quarantine or deleted;
- number of objects 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.

In order to save battery power, the backlight of the screen is automatically disabled by default during the scan. You can edit the settings of the screen's backlight (see the "Managing the backlight" section on page 115).

STARTING A SCHEDULED SCAN

You can configure automatic startup of the file system scan upon a schedule. A scheduled scan is carried out in background mode. When a malicious object is detected, the action selected in the Scan settings will be performed on it.

By default, starting a scheduled scan is disabled.

To set a scan schedule:

1. Select the **Scan** item in the **Anti-Virus** tab.

   This will open the **Scan** window.

2. Select the **Schedule** item.

This will open the **Schedule** screen.

3. Set the value for the **Auto scan** setting (see Figure below):

   - **Off**: disable scheduled scans.
   - **Weekly**: perform the scan once a week. Set the day and time for the scan to start. To do this, select values for the settings **Scan day** and **Scan time**.
   - **Daily**: perform the scan every day. In the **Scan time** field, apply the start time.

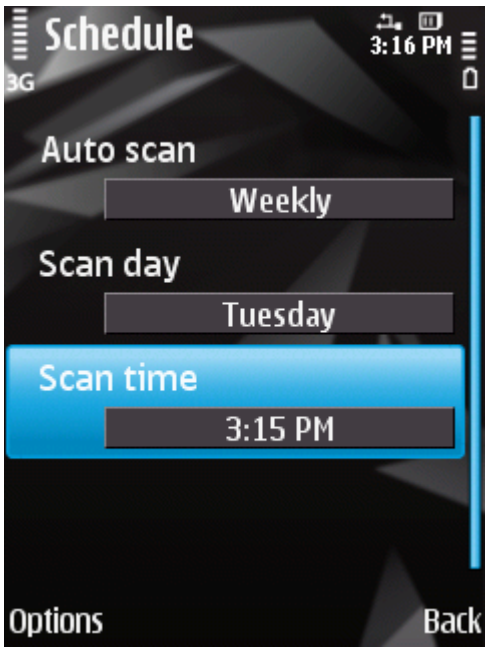


Figure 21: Configuration of starting a full scan on schedule

4. Press **Back** to save the changes.

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 edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To select objects to be scanned:

1. Select **Scan** in the **Anti-Virus** tab.

   This will open the **Scan** window.

2. Select **Objects / actions**.

   This will open the **Objects and actions** window.

3. Select a value for the **Objects to be scanned** settings (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.

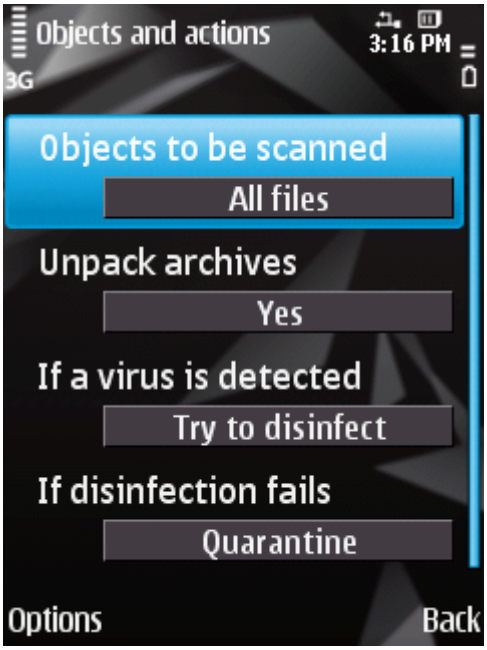


Figure 22: Selecting the object type scanned

4. Press **Back** to save the changes.

CONFIGURING ARCHIVE SCANS

Viruses often hide in archives. The program scans the following archive formats: ZIP, JAR, JAD, SIS and SISX. 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 edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To disable scan of archives:

1. Select the **Scan** item in the **Anti-Virus** tab.

   This will open the **Scan** window.

2. Select **Objects / actions**.

   This will open the **Objects and actions** window.

3. For the **Unpack archives** setting, select the value **No** (see Figure below).

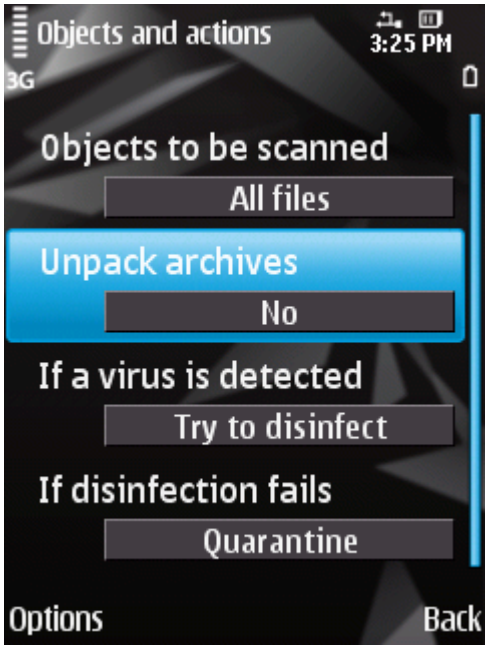


Figure 23: Configuring archive scans

4. Press **Back** to save the changes.

SELECTING THE ACTION TO BE PERFORMED ON DETECTED OBJECTS

By default, Kaspersky Mobile Security 9 places infected objects detected in quarantine. You can specify what actions the application will take when it detects a malicious object.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

1. Select the **Scan** item in the **Anti-Virus** tab.

   This will open the **Scan** window.

2. Select **Objects / actions**.

   This will open the **Objects and actions** window.

3. Set an action in respect of a malicious object. To do this, select a value for the **If a virus is detected** setting (see figure below):

   - **Delete**: delete detected malware objects without notifying the user.
   - **Quarantine**: quarantine detected malicious objects.
   - **Ask user**: prompt the user for action. When detecting a threat, open notification with a prompt for action.
   - **Log event**: 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).

- **Try to disinfect**: attempt to disinfect malware objects. If disinfection is not possible, the action specified for the **If disinfection fails** setting is performed.

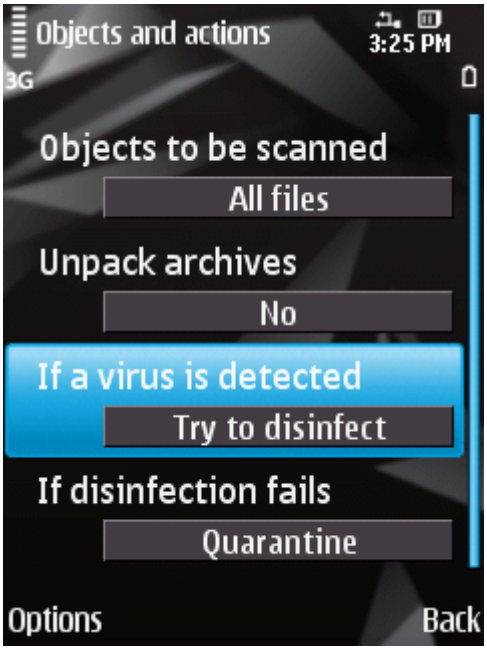


Figure 24: Selecting the action to be performed on malicious objects

4. If you selected **Try to disinfect**, set a second action for the application to take if the object cannot be disinfected. To do this, select a value for the **If disinfection fails** setting (see Figure below):

   - **Delete**: delete malware objects without notifying the user.
   - **Quarantine**: quarantine objects.
   - **Ask user**: prompt the user for actions when a malicious object is detected.
   - **Log event**: 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).

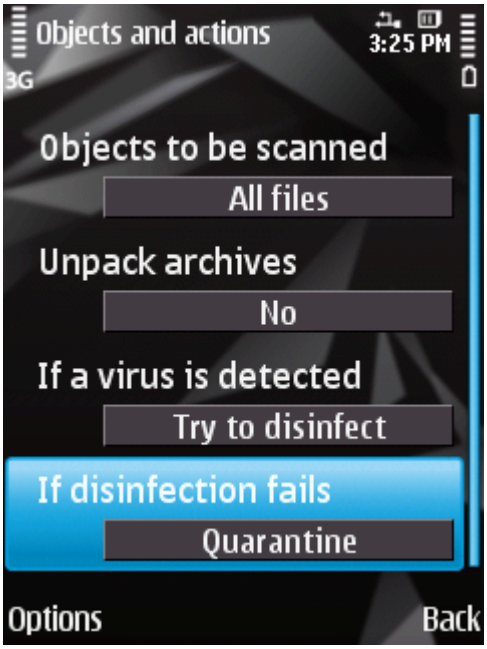


Figure 25: Selecting the action to be performed on malicious objects if disinfection is not possible

5. Press **Back** to save the changes.

RESTORING DEFAULT DEVICE SCAN SETTINGS

Initially, the application contains the settings recommended by Kaspersky Lab experts. When setting the device scan, you can always return to its recommended operation parameters.

To restore the default device scan settings:

1. Select the **Scan** item in the **Anti-Virus** tab.

   This will open the **Scan** window.

2. Select **Objects / actions**.

   This will open the **Objects and actions** window.

3. Select **Options** → **Restore**.

QUARANTINE OF POSSIBLY INFECTED OBJECTS

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

IN THIS SECTION

ABOUT QUARANTINE

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

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

VIEWING QUARANTINED OBJECTS

You can view objects placed in quarantine. For every object, its full name and date of detection are specified.

You can also view additional information about the infected object that you have selected: path to the object in the device before being moved to Quarantine by the application, and name of the threat.

- *To view the list of quarantined objects:*

  select the **Quarantine** item in the **Anti-Virus** tab.

This will open the **Quarantine** window, which contains a list of objects stored in Quarantine (see Figure below).

Figure 26: List of objects in quarantine

- *To view information about the object that you have selected,*

  select menu **Options** → **Details**.

  The following information will then be displayed on the screen: path to the file by which the application has detected it in the device, and name of the threat.

RESTORING OBJECTS FROM QUARANTINE

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

- *To restore an object from quarantine:*

  1. Select the **Quarantine** item on the **Anti-Virus** tab.

     This will open the **Quarantine** window.

  2. Select the object that you would like to restore, then select **Options** → **Restore**.

DELETING OBJECTS FROM QUARANTINE

You can delete one or all of the objects that have been placed in Quarantine.

- *To delete an object from Quarantine:*

  1. Select the **Quarantine** item in the **Anti-Virus** tab.

     This will open the **Quarantine** window.

  2. Select the object that you would like to delete, then select **Options** → **Delete**.

The selected object will be deleted.

To delete all quarantined objects:

1. Select the **Quarantine** item in the **Anti-Virus** tab.

   This will open the **Quarantine** window.

2. Select **Options** → **Delete all**.

All quarantined objects will be deleted.

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

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 63). According to the mode, Call&SMS Filter scans every incoming SMS or call and then determines whether this SMS or call is wanted or unwanted (spam). As soon as Call&SMS Filter assigns the wanted or unwanted status to an SMS or call, the scan is finished.

Information about blocked SMS and calls is registered in the application's log (see section "Application logs" on page 112).

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:

- **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.
- **Black list** – only calls and SMS originating from numbers on the Black List are allowed.
- **White list** – only calls and SMS originating from numbers on the White List are allowed.
- **Off** – all incoming calls and SMS are allowed.

You can change the Call&SMS Filter mode (see the "Changing the Call&SMS Filter mode" section on page 63). The current Call&SMS Filter mode is displayed on the **Call&SMS Filter** tab next to the menu item **Mode**.

CHANGING THE CALL&SMS FILTER MODE

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To change the mode of Call&SMS Filter:

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

   This will open the **Mode** window.

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

Figure 27: Changing the Call&SMS Filter mode

3. Press **Back** to save the changes.

CREATING THE BLACK LIST

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

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

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

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

Information about blocked SMS and calls is registered in the application's log (see section "Application logs" on page 112).

IN THIS SECTION

ADDING ENTRIES TO THE BLACK LIST

Bear in mind that the same number with identical filtering criteria cannot be included in the Black and White Lists of 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 edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

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

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

2. Select **Options** → **Add**.

3. Make the following settings (see Figure below):

   - **Block incoming** – type of event from a telephone number which Call&SMS Filter blocks for Black List numbers:
     - **Calls and SMS**: block incoming SMS messages and calls.
     - **Calls only:** block incoming calls only.

- **SMS only**: block incoming SMS messages only.

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

- **Containing text** – key phrase indicating that the received SMS message is unwanted (spam). Call&SMS Filter only blocks SMS containing the key phrase, while delivering all other SMS. The setting is available if for the **Block incoming** setting the **SMS only** value is set.

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

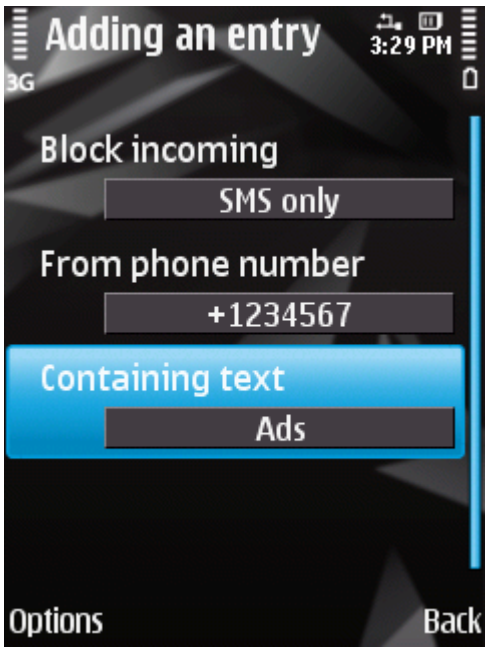


Figure 28: Settings for entries in the Black List

4. Press **Back** to save the changes.

EDITING ENTRIES IN THE BLACK LIST

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

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

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

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

2. Select the entry on the list that you want to edit and then select **Options** → **Change**.

3. Change the necessary settings of the entry:

- **Block incoming** – type of event from a telephone number which Call&SMS Filter blocks for Black List numbers:
  - **Calls and SMS**: block incoming SMS messages and calls.
  - **Calls only**: block incoming calls only.
  - **SMS only**: block incoming SMS messages only.
- **From phone number** – telephone number for which Call&SMS Filter blocks incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any amount of symbols, and "?" any one symbol). For example, *1234? on the Black List. Call&SMS Filter blocks calls or SMS from a number in which any symbol follows the figure 1234.
- **Containing text** – key phrase indicating that the received SMS message is unwanted (spam). Call&SMS Filter only blocks SMS containing the key phrase, while delivering all other SMS. The setting is available if for the **Block incoming** setting the **SMS only** value is set.

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

4. Press **Back** to save the changes.

DELETING ENTRIES FROM THE BLACK LIST

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

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

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

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

2. Select the entry on the list that you want to delete and then select **Options** → **Delete**.

To clear the Call&SMS Filter Black List:

1. On the **Call& SMS Filter** tab, select **Black List**.
2. This will open the **Black List** window.
3. Select **Options** → **Delete all**.

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

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 edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

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

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

2. Select **Options** → **Add**.

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

   - **Allow incoming** – type of event from a telephone number which Call&SMS Filter allows for Black List numbers:
     - **Calls and SMS**: allow incoming calls and SMS messages.
     - **Calls only**: allow incoming calls only.
     - **SMS only**: allow incoming SMS messages only.
   - **From phone number**: telephone number for which Call&SMS Filter blocks incoming information.. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any amount of symbols, and "?" any one symbol). For example, *1234? in the White List. Call&SMS Filter delivers calls or SMS from a number in which any symbol follows the figure 1234.
   - **Containing text** – key phrase indicating that the received SMS message is wanted. For numbers on the White List, Call&SMS Filter only delivers SMS messages containing the key phrase and blocks all others. The setting is available if for the **Allow incoming** setting the **SMS only** value is set.

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

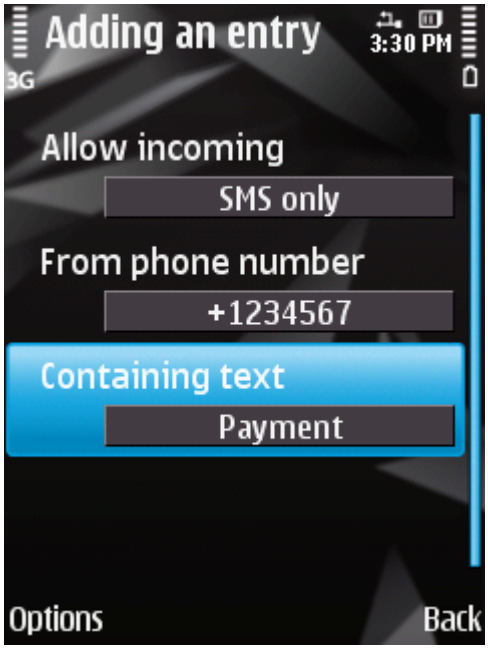


Figure 29: Settings for entries in the White List

4. Press **Back** to save the changes.

EDITING ENTRIES IN THE WHITE LIST

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

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To edit an entry on the Call&SMS Filter White List:

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

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

2. Select the entry on the list that you want to change and then select **Options** → **Change**.

3. Change the necessary settings of the 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.
   - **From phone number**: telephone number for which Call&SMS Filter blocks incoming information.. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any amount of symbols, and "?" any one symbol). For example, *1234? in the White List. Call&SMS Filter delivers calls or SMS from a number in which any symbol follows the figure 1234.

- **Containing text** – key phrase indicating that the received SMS message is wanted. For numbers on the White List, Call&SMS Filter only delivers SMS messages containing the key phrase and blocks all others. The setting is available if for the **Allow incoming** setting the **SMS only** value is set.

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

4. Press **Back** to save the changes.

DELETING ENTRIES FROM THE WHITE LIST

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

To delete an entry from the Call&SMS Filter White List:

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

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

2. Select the entry on the list that you want to delete and then select **Options** → **Delete**.

To clear the Call&SMS Filter White List:

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

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

2. Select **Options** → **Delete all**.

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

If the **Both lists** or **White List** modes are selected for Call&SMS Filter, you can additionally set a response from Call&SMS Filter to SMS and calls from subscribers, whose numbers are not saved in Contacts. In addition, Call&SMS Filter allows expansion of the White List by adding numbers from the list of contacts to it.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

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

   This will open the **Mode** window.

2. Select one of the values for the **Allow Contacts** setting (see Figure below):

   - In order for Call&SMS Filter to regard numbers from the phone book as an additional White List, select the **Yes** value;

   - in order for Call&SMS Filter to filter SMS messages and calls based on the Call&SMS Filter mode set, select the **No** value.

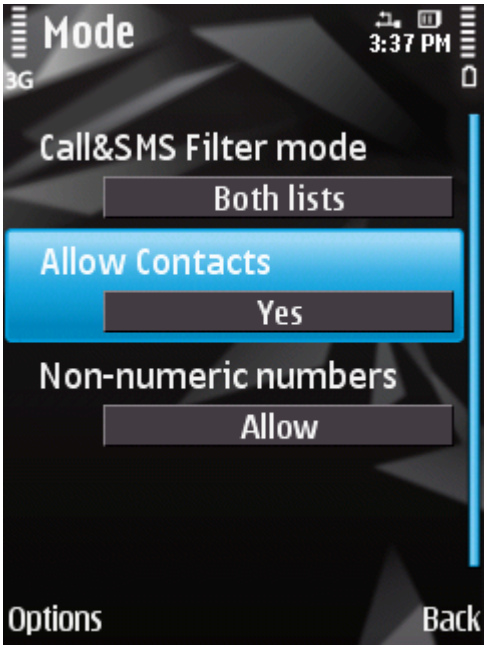


Figure 30: Call&SMS Filter response to numbers not included in the device's phone book

3. Press **Back** to save the changes.

RESPONDING TO SMS MESSAGES FROM NON-NUMERIC NUMBERS

If the **Both lists** or **Black List** modes are selected for Call&SMS Filter, you can additionally expand the Black List by including all non-numeric numbers (those containing letters). Then Call&SMS Filter will block SMS messages from non-numeric numbers.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

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

   This will open the **Mode** window.

2. Select a value for the **Non-numeric numbers** setting (see Figure below):

   - In order for Call&SMS Filter to automatically delete SMS messages from non-numeric numbers, select the **Block** value.
   - In order for Call&SMS Filter to filter SMS messages from non-numeric numbers only on the basis of the Anti-Spam mode set, select the **Allow** value.

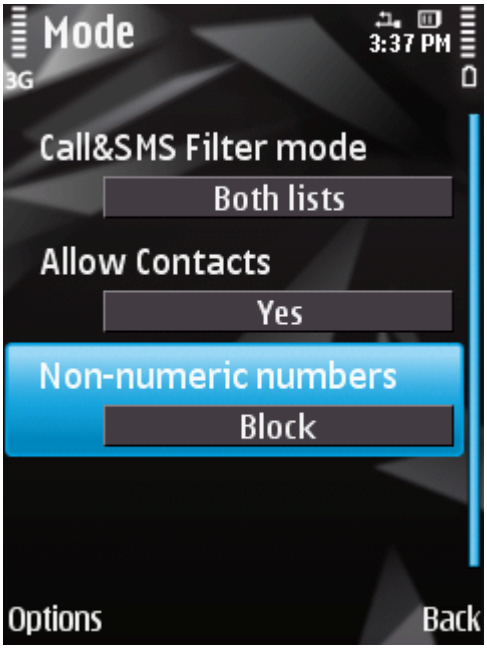


Figure 31: Configuring Call&SMS Filter action when receiving SMS messages from non-numeric numbers

3. Press **Back** to save the changes.

SELECTING A RESPONSE TO INCOMING SMS

In **Both lists** mode, Call&SMS Filter compares incoming SMS against entries on the Black List and White List.

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.

You can select one of the following actions to be taken in respect of the SMS message (see figure below):

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

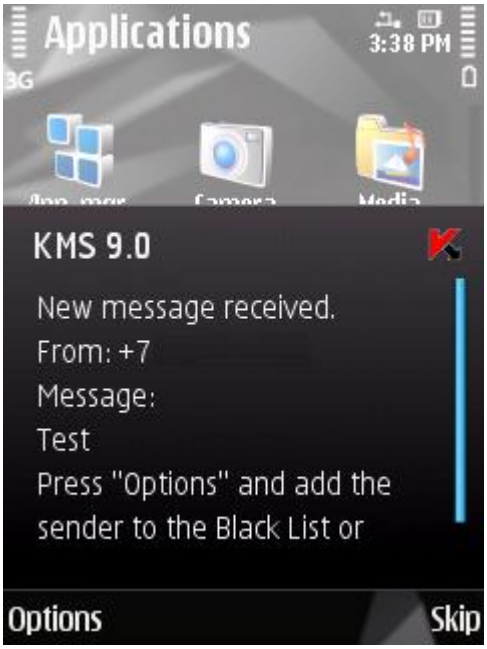


Figure 32: Call&SMS Filter notification about the receipt of an SMS

Information about blocked SMS messages is entered in the application log (see the "Application logs" section on page 112).

SELECTING RESPONSE TO INCOMING CALLS

In **Both lists** mode, Call&SMS Filter compares incoming calls against entries on the Black List and White List.

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.

You can select one of the following actions for the number from which the call was made (see Figure below):

- To add the caller's telephone number to the Black List, select **Options** → **Add to Black List**.
- To add the caller's telephone number to the White List, select **Options** → **Add to White List**.
- **Skip**: do not add the caller's number to either list.

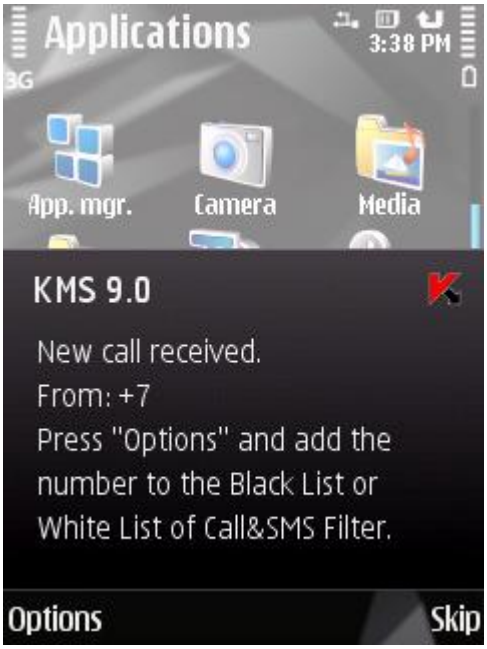


Figure 33: Call&SMS Filter notification about an accepted call

Information about blocked calls is entered in the application's log (see the "Application logs" section on page 112).

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.

IN THIS SECTION

ABOUT PARENTAL CONTROL

Parental Control enables the control of outgoing SMS messages and calls based on the Black and White Lists of subscribers' numbers. The component's operation is ruled by the mode.

In **Black List** mode, Parental Control blocks outgoing SMS messages or calls addressed to numbers on the Black List while allowing those addressed to any other numbers. In **White List** mode, Parental Control only allows outgoing SMS messages and calls addressed to numbers on the White List while blocking those addressed to any other numbers. In **Off** mode, Parental Control does not deal with outgoing SMS messages and calls.

Parental Control blocks outgoing SMS messages if they are sent using the device’s standard features only. Parental Control allows outgoing SMS messages if they are sent using third-party applications.

Information about the component's operation is entered in the application's log (see the "Application Logs" section on page 112).

PARENTAL CONTROL MODES

The Parental Control mode determines the rule, which defines the control of outgoing SMS messages and calls.

The following Parental Control modes are available:

- **Off** - disable Parental Control. Do not control outgoing SMS messages and calls.

  This mode is selected by default.

- **Black List** – block the sending of SMS and / or calls only to numbers on the Black List, while allowing any other SMS messages and calls.

- **White List** – allow the sending of SMS and / or calls only to numbers on the White List, while blocking any other SMS messages and calls.

You can edit the Parental Control mode (see the "Changing the Parental Control mode" section on page 75).

The current Parental Control operating mode is displayed on the **Parental Control** tab next to the **Mode** menu item.

CHANGING THE PARENTAL CONTROL MODE

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To change the Parental Control mode:

1. On the **Parental Control** tab, select **Mode**.

   This will open the **Mode** window.

2. Select one of the Parental Control modes suggested (see Figure below).

Figure 34: Changing the Parental Control mode

3. Press **OK** to save the changes.

CREATING THE BLACK LIST

You can create a Black List that Parental Control should use to block outgoing SMS messages and calls. The list contains telephone numbers to which the sending of SMS and calls is not blocked.

Information about blocked SMS messages and calls is registered in the application's log (see the "Application logs" section on page 112).

IN THIS SECTION

ADDING ENTRIES TO THE BLACK LIST

Bear in mind that the same number with identical filtering criteria cannot be included in the Black and White Lists of Parental Control numbers at the same time. If a number with such criteria is already saved on either of the lists, Kaspersky Mobile Security 9 will notify you of this event, and the relevant message will appear on the screen.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To add an entry to the Parental Control Black List:

1. On the **Parental Control** tab, select **Black List**.

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

2. Select **Options** → **Add**.

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

   - **Block outgoing**: type of outgoing information from a subscriber number which Parental Control blocks:
     - **SMS and calls**: block outgoing calls and SMS messages.
     - **Calls only**: block outgoing calls only.
     - **SMS only**: block outgoing SMS messages only.
   - **Phone number**: the phone number which is blocked for outgoing SMS messages and/or calls. 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).

Figure 35: Settings for entries in the Black List

4. Press **Back** to save the changes.

EDITING ENTRIES IN THE BLACK LIST

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

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To edit an entry in the Parental Control Black list:

1. On the **Parental Control** tab, select **Black List**.

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

2. Select the entry on the list that you want to edit and then select **Options** → **Change**.

3. Change the necessary settings of the entry:

   - **Block outgoing**: type of outgoing information from a subscriber number which Parental Control blocks:
     - **SMS and calls**: block outgoing calls and SMS messages.
     - **Calls only**: block outgoing calls only.
     - **SMS only**: block outgoing SMS messages only.
   - **Phone number**: the phone number which is blocked for outgoing SMS messages and/or calls. 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).

4. Press **Back** to save the changes.

DELETING ENTRIES FROM THE BLACK LIST

It is possible that a number is accidentally added to the Black list of blocked numbers list. You can delete such a number from the list.

To delete an entry from the Parental Control Black List, perform the following steps:

1. On the **Parental Control** tab, select **Black List**.

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

2. Select the entry on the list that should be deleted and then select **Options** → **Delete**.

DELETING ALL ENTRIES FROM THE BLACK LIST

To delete all entries from the Parental Control Black List, perform the following steps:

1. On the **Parental Control** tab, select **Black List**.

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

2. Select **Options** → **Delete all**.

The list is emptied.

CREATING A WHITE LIST

You can create a White list on the basis of which Parental Control allows sending SMS and calls.

The list contains phone numbers to which Parental Control allows sending SMS messages and calls.

Information about blocked SMS messages and calls is registered in the application's log (see the "Application logs" section on page 112).

IN THIS SECTION

ADDING ENTRIES

Bear in mind that the same number with identical filtering criteria cannot be included in the Black and White Lists of Parental Control numbers at the same time. If a number with such criteria is already saved on either of the lists, Kaspersky Mobile Security 9 will notify you of this event, and the relevant message will appear on the screen.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To add an entry to the Parental Control White List:

1. On the **Parental Control** tab, select **White List**.

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

2. Select **Options** → **Add**.

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

   - **Allow outgoing**: type of outgoing information which Parental Control allows to be sent to a subscriber number:
     - **SMS and calls**: allow outgoing calls and SMS messages.
     - **Calls only:** allow outgoing calls only.
     - **SMS only**: allow outgoing SMS messages only.
   - **Phone number**: the phone number to which outgoing SMS messages and / or calls are allowed by the Parental Control. 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).

Figure 36: Settings for entries in the White List

4. Press **Back** to save the changes.

EDITING ENTRIES IN THE WHITE LIST

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

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To edit an entry in the Parental Control White list:

1. On the **Parental Control** tab, select **White List**.

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

2. Select the entry on the list that you want to edit and then select **Options** → **Edit**.

3. Change the necessary settings of the entry:

   - **Allow outgoing**: type of outgoing information which Parental Control allows to be sent to a subscriber number:

     - **SMS and calls**: allow outgoing calls and SMS messages.

     - **Calls only:** allow outgoing calls only.

     - **SMS only**: allow outgoing SMS messages only.

   - **Phone number**: the phone number to which outgoing SMS messages and / or calls are allowed by the Parental Control. 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).

4. Press **Back** to save the changes.

DELETING ENTRIES FROM THE WHITE LIST

It is possible that a number is accidentally added to the White List. You can delete a number from the list created.

To delete an entry from the Parental Control White List:

1. On the **Parental Control** tab, select **White List**.

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

2. Select the entry on the list that you want to delete and then select **Options** → **Delete**.

DELETING ALL ENTRIES

To delete all entries from the Parental Control White List:

1. On the **Parental Control** tab, select **White List**.

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

2. In the **Options** → **Delete all** menu.

The list is emptied.

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

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

Anti-Theft includes the following functions:

- **Block** – allows blocking the device remotely and gives the text to be displayed on the screen of the blocked device.
- **Data Wipe** – can remotely delete the user's personal data from the device (entries in Contacts, SMS, picture gallery, calendar, logs, Internet connection settings) and information from the storage cards, folders from list for deletion.
- **SIM Watch** allows obtaining the current phone number in the event that the SIM card is replaced, as well as locking the device in the event the SIM card is replaced or the device is activated without a SIM card. Information about a new telephone number is sent as a message to a phone number and / or email that you specified.
- The **GPS Find** functionality enables you to locate a device. The geographical coordinates of the device are sent as a message to the phone number from which a special SMS command was sent, and to an email address.

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

Kaspersky Mobile Security 9 can remotely start Anti-Theft with sending SMS commands from another mobile device (see "Remote start of the Anti-Theft functions" on page 90).

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

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

Information about the component's operation is stored in the component log (see section "Application logs" on page 112).

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 edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To enable the Block function:

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

   This will open the **Block** window.

2. Select the **On** value for the **Block mode** setting.

3. In order to display text on the screen of a blocked device, select the **Text when blocked** item and fill in the **Enter text** field (see Figure below). When the device is blocked, the text Device Blocked is displayed on the screen by default.

   To prevent the text from being displayed, select the **Text when blocked** setting and then delete the contents of the **Enter text** field and press **OK**.

Figure 37: Block function settings

4. Press **Back** to save the changes.

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

- Use a Kaspersky Lab mobile application, such as Kaspersky Mobile Security 9, on another mobile device to create and send an SMS command to your device. To create a special SMS command, use the **Send command** function. As a result, your device will receive a covert SMS, and the device will be blocked.

- On another mobile device, create and send an SMS with the special text and the secret code previously set for the receiving device. As a result, your device will receive a covert SMS, and the device will be blocked.

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

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

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

1. On the **Additional** tab, select **Send menu**.

   The screen designed for sending a special command opens.

2. Press **Start**.

3. Select the **Block** command type and then press **Next** (see figure below).

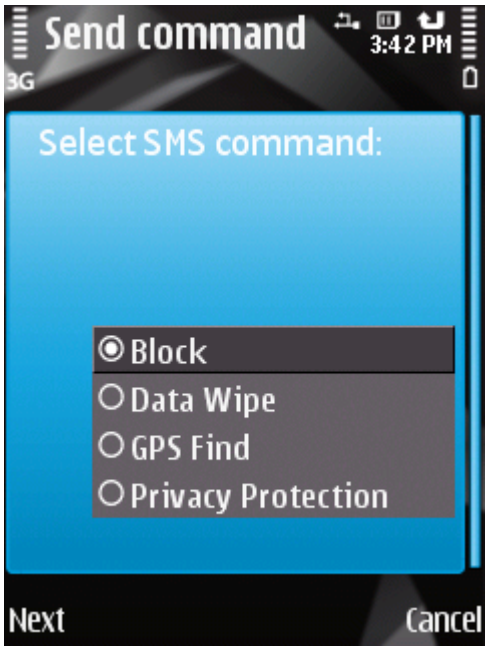


Figure 38: Remote device blocking

4. Enter the phone number of another device that receives the SMS command, and press **Next**.

5. Enter the secret code of the application specified on the device that receives the SMS command, and 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:

- user's personal data (entries in Contacts and on SIM card, SMS messages, gallery, calendar, Internet connection settings);
- information on storage card;
- files from the **C:\Data** folder and other folders on the **Folders to be deleted** list.

This function does not delete data stored on the device, but it simply enables the option to delete them after a special SMS command is received.

To enable the Data Wipe function:

1. Select the **Anti-Theft** tab, select **Data Wipe**.

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

2. Select the **Mode** item.

   This will open the **Mode** window.

3. Select the **Data Wipe mode** item and set the **On** value (see Figure below).

4. Select data to be deleted when the device receives a special SMS command:

   - to delete personal details, install for the **Delete personal data** the value **Yes**;
   - to delete files from the **C:\Data** folder and from the **Folders to be deleted** list, set **Delete folders** to **Yes**.

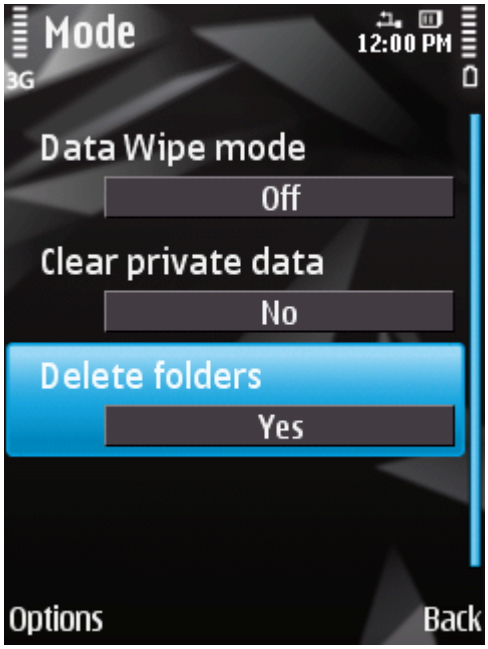


Figure 39: Data Wipe function settings

5. Press **Back** to save the changes.

6. Proceed with creating the **Folders to be deleted** list (see section "**Creating a list of folders to delete**" on page 86).

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 an 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. On the **Additional** tab, select **Send menu**.

   The screen designed for sending a special command opens.

2. Press **Start**.

3. Select the **Data Wipe** command type and then press **Next** (see figure below).

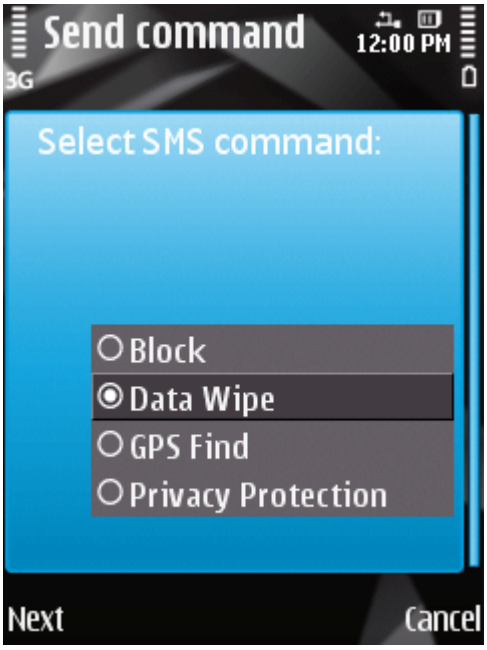


Figure 40: Deleting personal data

4. Enter the phone number of the device that receives the SMS command, and press **Next**.

5. Enter the secret code of the application specified on the device that receives the SMS command, and click **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 folders from the list after a special SMS command is received, make sure that the **Yes** value is set for the **Delete folders** option in the **Mode** menu item on the **Anti-Theft** tab.

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

1. Select the **Anti-Theft** tab, select **Data Wipe**.

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

2. Select the **Folders to be del.** item.

   This will open the **Folders to be deleted** screen.

3. Select **Options** → **Add** (see figure below).

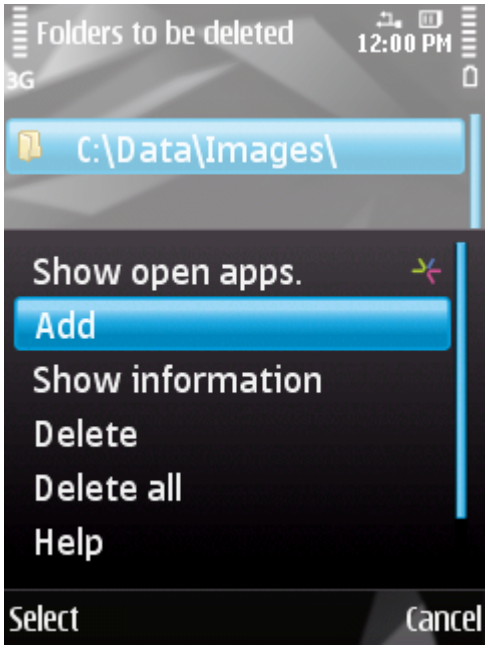


Figure 41: Adding folders

4. Select the necessary folder from the folder tree and press **OK**.

   The folder is added to the list.

5. Press **Back** to save the changes.

To remove a folder from the list:

1. Select the **Anti-Theft** tab, select **Data Wipe**.

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

2. Select the **Folders to be del.** item.

   This will open the **Folders to be deleted** screen.

3. Select a folder from the list and then select **Options** → **Delete**.

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

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 check the replacement of the SIM card:

1. Select the SIM Watch item on the **Anti-Theft** tab.

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

2. Select **SIM Watch mode** and set the **On** value.

3. Configure the following SIM-Watch settings (see Figure below):

   - **Message to email**. To obtain an e-mail with the new number of your phone, enter an e-mail address.
   - **SMS to number**. To automatically receive an SMS with your telephone's new number, enter the telephone number to which the SMS should be sent. The phone number may begin with a digit or with a "+", and must contain digits only.
   - **Block device**. To block the device if the SIM card is replaced or if the device is turned on without it, set to **Yes**. You can unblock the device only by entering the secret code. By default, blocking the device is disabled.
   - **Text when blocked**. To display a message on the screen in blocked mode, enter it in the **Enter text** field. By default, the standard text in which you can add the owner's number is used for the message.

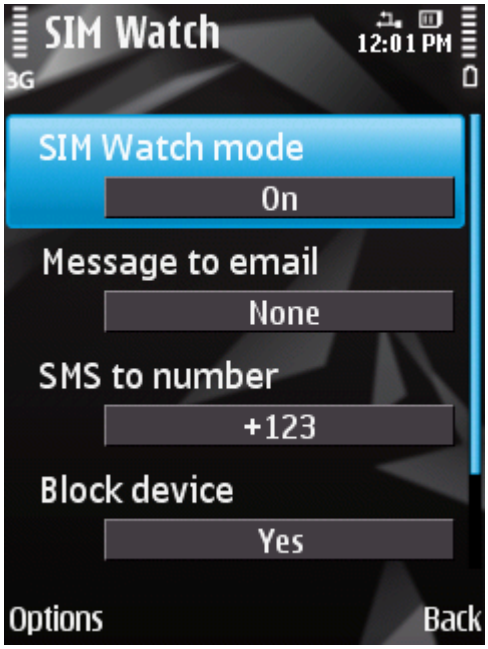


Figure 42: SIM Watch function settings

4. Press **Back** to save the changes.

DETERMINING THE DEVICE'S GEOGRAPHICAL COORDINATES

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

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

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

To enable the GPS Find function:

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

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

2. Set the **On** value for the **GPS Find mode** option.

3. For the **Message to email** setting, enter the email address to which the device's geographical coordinates should be sent (see figure below).

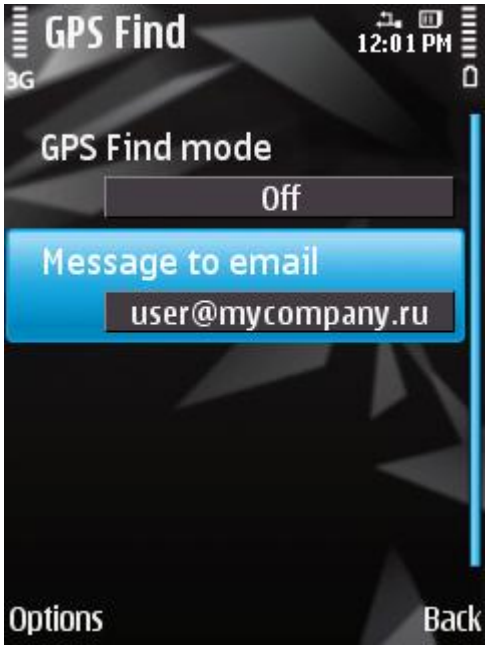


Figure 43: GPS Find function settings

4. Press **Back** to save the changes.

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

- Use a Kaspersky Lab mobile application, such as Kaspersky Mobile Security 9, on another mobile device to create and send an SMS command to your device. As a result, your device will receive a covert SMS, and the application will send the device's coordinates. To create a special SMS command, use the Sending a command function.

- On another mobile device, create and send an SMS with the special text and the secret code previously set for the receiving device. As a result, your device will receive a covert SMS, and the application will send the device's coordinates.

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

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

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

1. On the **Additional** tab, select **Send menu**.

   The screen designed for sending a special command opens.

2. Select the command type **GPS Find** and then press **Next** (see Figure below).

Figure 44: Determine the location of the device

3. Enter the phone number of another device that receives the SMS command, and press **Next**.

4. Enter the secret code of the application specified on the device that receives the SMS command, and 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 `find:<code>`, where `<code>` is the application secret code set on another device. The message is not case sensitive, and spaces before or after the colon are ignored.

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

STARTING ANTI-THEFT FUNCTIONS REMOTELY

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

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

To send an SMS command to another device:

1. Select the **Additional** tab, select **Send menu**.

   The screen designed for sending a special command opens.

2. Press **Start**.

3. Select one of the suggested functions to be started remotely (see Figure below):

- **Block** (see "**Blocking the device**" section on page 82).
- **Data Wipe** (see "**Deleting personal data**" section on page 84).
- **GPS Find**.
- **Privacy Protection** (see "**Privacy Protection**" section on page 92).

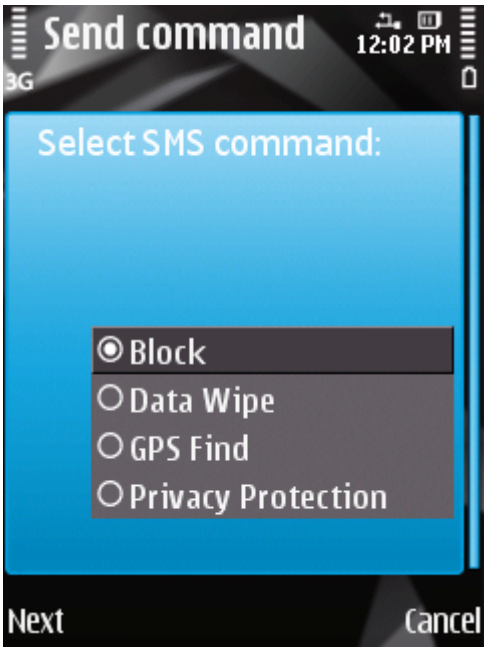


Figure 45: Remote start of Anti-theft functions

The function that you want to use should be enabled on the device that receives an SMS command.

4. Press **Next**.
5. Enter the phone number of another device that receives the SMS command, and press **Next**.
6. Enter the secret code specified on the device that receives the message, and press **Send**.

PRIVACY PROTECTION

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

IN THIS SECTION

PRIVACY PROTECTION

Privacy Protection hides private data 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.

Information about the operation of Privacy Protection is stored in the log (see "Application logs" section on page 112).

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:

- **Normal** – private data are displayed. The Privacy Protection settings are accessible for modification.
- **Private** – private data are hidden. The Privacy Protection settings cannot be changed.

You can configure automatic enabling (see section "Enabling Privacy Protection automatically" on page 93) of Privacy Protection or remote enabling from another device (see section "Enabling Privacy Protection remotely" on page 94).

The component's current status is displayed on the **Privacy Protection** tab next to the **Mode** item.

Changing the mode of Privacy Protection can take some time.

CHANGING THE PRIVACY PROTECTION MODE

The Privacy Protection mode can be changed as follows:

- from the application interface;
- with the secret code when the device is in active waiting mode.

To change the Privacy Protection mode:

1. Select the **Mode** item on the **Privacy Protection** tab.

   The **Privacy Protection mode** window opens.

2. Select a value for the setting **Privacy Protection mode** (see Figure below).

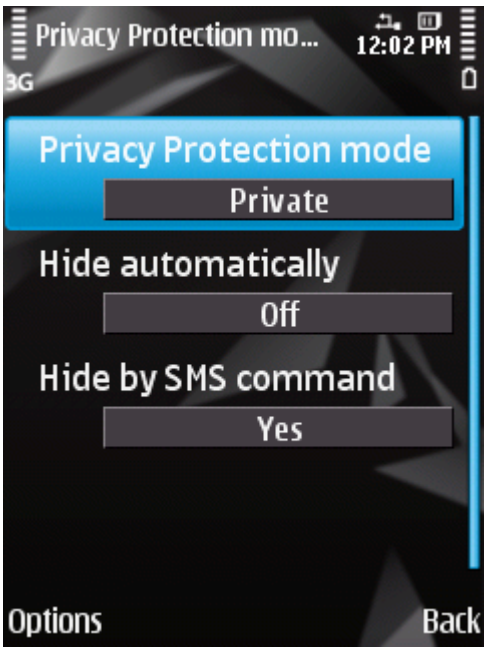


Figure 46: Changing Privacy Protection mode

3. Press **Back** to save the changes.

To change the Privacy Protection mode with the secret code when the device is in active waiting mode,

enter the ***secret code#**.

When the Privacy Protection mode is changed, a notification appears on the device's screen.

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. Select the **Mode** item on the **Privacy Protection** tab.

   The **Privacy Protection mode** window opens.

2. Select a value for the time interval, which should enable Privacy Protection, when elapsed. To do this, set one of the suggested values for the **Hide automatically** setting (see Figure below).

   - **No delay**.
   - **After 1 minute**.
   - **After 5 minutes**.
   - **After 15 minutes**.
   - **After 1 hour**.
   - **Off**

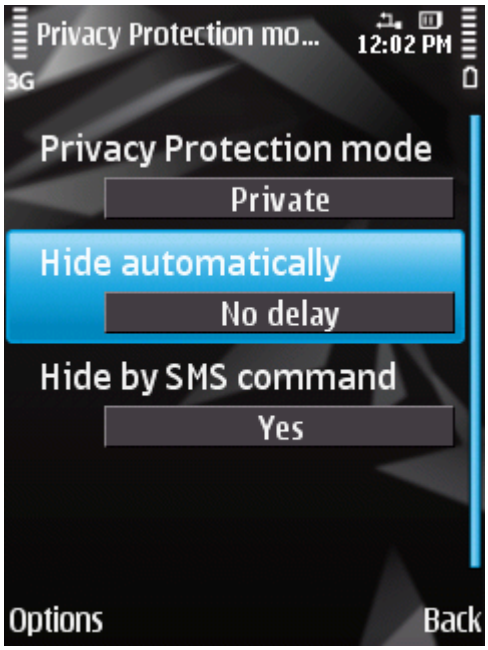


Figure 47: Automatic start of Privacy Protection

3. Press **OK** to save the changes.

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. Select the **Mode** item on the **Privacy Protection** tab.

The **Privacy Protection mode** window opens.

2. For **Hide on SMS command**, select **Yes** (see figure below).

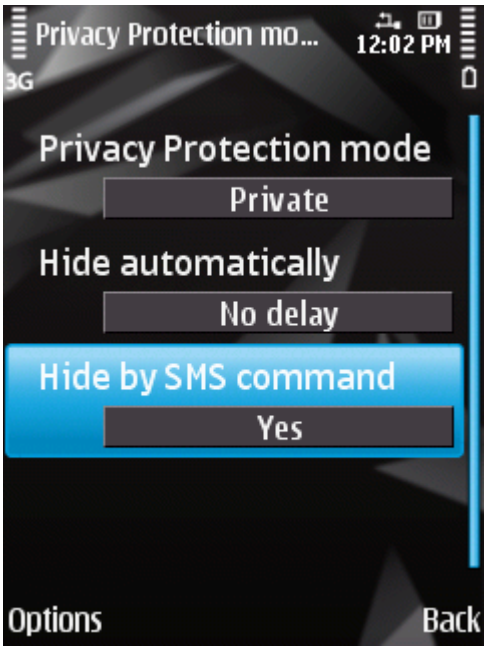


Figure 48: Privacy Protection remote enabling settings

3. Press **Back** to save the changes.

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 enable Privacy Protection remotely using a special SMS command:

1. On the **Additional** tab, select **Send menu**.

   The screen designed for sending a special command opens.

2. Press **Start**.

3. Select the **Privacy Protection** command type and press **Next** (see figure below).

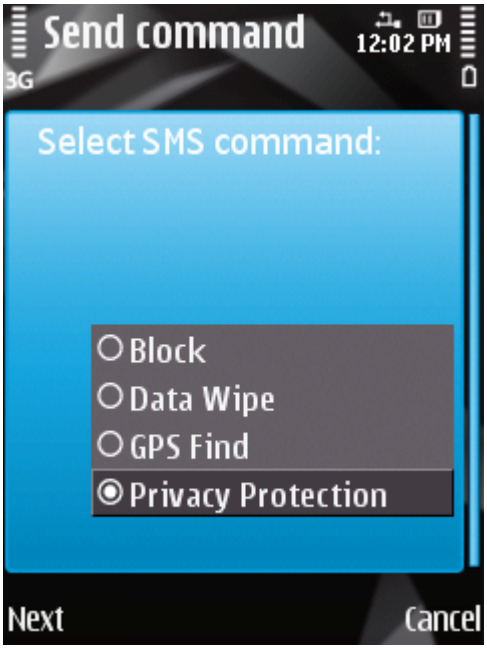


Figure 49: Privacy Protection remote start

4. Enter the phone number of the device that receives the SMS command, and press **Next**.

5. Enter the secret code of the application specified on the device that receives the SMS command, and press **Send**.

When the device receives the SMS command, it enables Privacy Protection automatically.

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

sendan 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.

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

You can add a number manually (for example, +12345678), import a number from Contacts or SIM card.

Before making the Contact List, disable hiding confidential information.

To add an entry to the Contact List:

1. Select **Privacy Protection** on the **Contact list** tab.

   The **Contact list** window will open.

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

   - To add a number manually, select **Options** → **Add** → **Number**. In the **Number** window that opens, fill in the **Enter phone number** field. On completion of the entry, press **OK**.
   - To add a number from Contacts, select **Options** → **Add** → **Contacts**. Then on the **Contacts** screen that opens, select the required contact from the phone book using the **Options** → **Select** menu. On completion of the entry, press **OK**.
   - To add a number saved on the SIM card, select **Options** → **Add** → **Contact from SIM**. In the **Contacts from SIM** window that opens, select the required number from the list of numbers on the SIM card using the **Options** → **Select** menu. On completion of the entry, press **OK**.

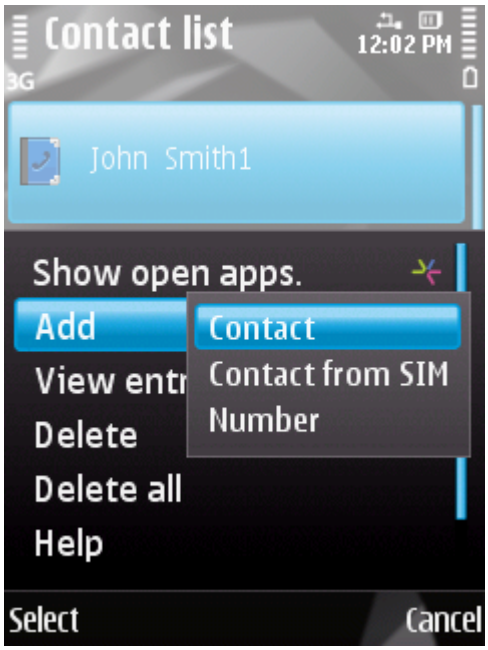


Figure 50: Adding entries to the list of protected contacts

3. Press **Back** to save the changes.

EDITING A NUMBER IN THE LIST OF PRIVATE NUMBERS

Phone numbers added manually are only available for editing on the Contact List. It is not possible to edit numbers which are selected from the phone book or numbers list on the SIM card.

Before making the Contact List, disable hiding confidential information.

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

1. Select the **Privacy Protection** tab, select **Contact list**.

   The **Contact list** window will open.

2. Select a number to be edited from the Contact List and then select **Options** → **Change**.

   The phone number of the selected contact appears on the screen.

3. Change the data in the **Enter phone number** field.

4. When completing the editing, press **OK**.

DELETING A NUMBER FROM THE LIST OF PRIVATE NUMBERS

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

Before making the Contact List, disable hiding confidential information.

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

1. Select the **Privacy Protection** tab, select **Contact list**.

   The **Contact list** window will open.

2. Select a number from the list and then select **Options** → **Delete**.

3. Confirm deletion. To do this, press **Yes**.

- *To clear the Contact List:*

1. Select the **Privacy Protection** tab, select **Contact list**.

   The **Contact list** window will open.

2. Select **Options** → **Delete all**.

3. Confirm deletion. To do this, press **Yes**.

The Contact List becomes empty.

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. Select the item **Hidden Objects** on **Privacy objects**.

   This will open the **Hidden objects** screen.

2. Select objects to be hidden for protected numbers. For every setting required, set to **Hide** using **Options** → **Change**. The component provides the option to hide the following information (see figure below):

   - **Contacts** – hide all information about confidential numbers in the Contacts.
   - **Messages** – hide SMS messages in the **Incoming**, **Outgoing** and **Sent** folders for confidential numbers.
   - **Call entries** - 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.
   - **Incoming SMS** – do not display the delivery of incoming SMS messages (there is no message of receipt of a new SMS message from a confidential number). All SMS messages received from private numbers will be displayed for viewing when Privacy Protection is disabled.

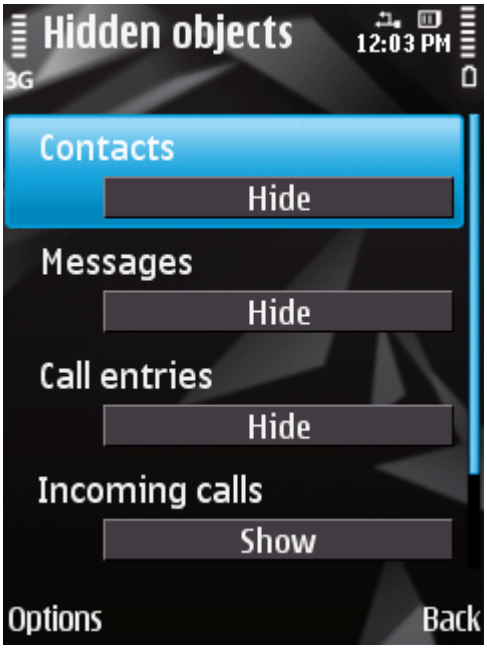


Figure 51: Selecting hidden objects

3. Press **Back** to save the changes.

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.

IN THIS SECTION

ABOUT FIREWALL

Firewall monitors your device's network connections based on the selected mode. Firewall allows you to set permitted connections (for example, to perform synchronization with the remote administration system) and blocked connections (for example, Internet search, file download).

After installation, Kaspersky Mobile Security 9 Firewall is disabled.

The Firewall enables the setting of notifications about blocked connections (see the "Notifying of a connection attempt" section on page 101).

Information about the operation of the Firewall is entered in the application's log (see the "Application logs" section on page 112).

ABOUT FIREWALL SECURITY LEVELS

You can select the mode in accordance with which the Firewall determines the permitted and blocked connections. The following Firewall modes are available:

- **Off** any network activity is permitted.
- **Only incoming connections are blocked**: block incoming connections only. Outgoing connections are allowed.
- **Outgoing connections using SSH, HTTP, HTTPS, IMAP, SMTP and POP3 protocols are allowed**: block all incoming connections. Checking e-mails, viewing websites and downloading files is accessible Outgoing connections can only be established using SSH, HTTP, HTTPS, IMAP, SMTP, POP3 ports.
- **Block all**: block all network activity, except for updating the application databases and renewing the license.

You can change the Firewall mode (see "Selecting Firewall security level" on page 101). The current mode is displayed on the **Firewall** tab next to the **Mode** menu item.

SELECTING FIREWALL SECURITY LEVEL

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To set Firewall mode:

1. Select the **Mode** item on the **Firewall** tab.

   This will open the **Mode** window.

2. Select one of the Firewall modes offered. To do so, move the cursor to the name of the required mode (see figure below).

Figure 52: Firewall mode selection

3. Press **OK** to save the changes.

NOTIFYING OF A CONNECTION ATTEMPT

The Firewall blocks all banned connections on the basis of the mode selected (see Firewall security level selection section on page 101). For the Firewall to inform you of blocked connections on the mobile device, apply the setting to receive Firewall notifications.

To set the Firewall so that you receive notifications about blocking:

1. Select the **Notifications** item on the **Firewall** tab.

2. For **If connection is blocked** select one of the following values (see figure below):

   - **Notify** – enable delivery of notifications. Firewall notifies of a blocked connection.

- **Do not notify** – disable delivery of notifications. Firewall does not notify you of a blocked connection.

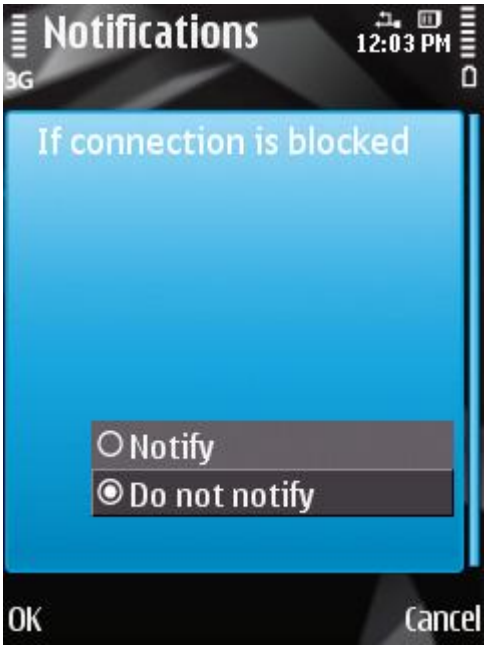


Figure 53: Configuring Firewall notifications

3. Press **OK** to save the changes.

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.

IN THIS SECTION

ABOUT ENCRYPTION

Encryption encrypts data in your list of folders to encrypt. The Encryption function operation is based on the action of the function of the same name that is built into the operating system of your device. The Encryption function allows encrypting any type of folder with the exception of system folders. You can select folders to be encrypted in the device's memory or on a storage card. To gain access to encrypted data, enter the application PIN code set when the application was first run.

To run executables out of an encrypted folder, you must first decrypt the folder. This requires that the application PIN code be entered first.

To gain access to encrypted data, you need to enter the secret code. You can create a time interval (see "Blocking access to encrypted data" on page 105), in which access to encrypted folders is blocked and which require the secret code to be entered. The function becomes activated after the device switches to power-saving mode.

After installing Kaspersky Mobile Security 9, the Encryption component is disabled.

Information about the component's operation is entered in the application's log (see the "Application Logs" section on page 112).

ENCRYPTING DATA

Encryption allows encrypting any number of non-system folders which are in the device memory or on a storage card.

The list of all previously encrypted and decrypted files is accessible in the **Encryption** window from the **Folders list** menu item.

You can also encrypt one or all of the folders in the folders list immediately.

To add a folder to the list of folders for encryption and encrypt it:

1. Select the **Folders list** item on the **Encryption** tab.

   This will open the **Folders list** window.

2. Select **Options** → **Add** (see figure below).

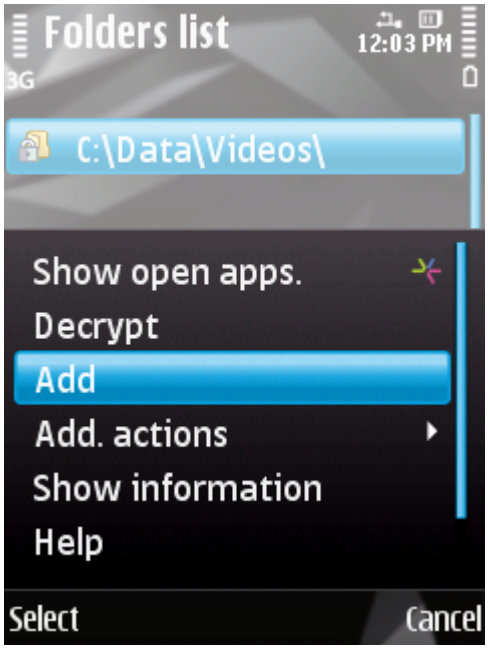


Figure 54: Data encryption

A screen will open with the system file tree of your device.

3. Select the folder to be encrypted and then start the encryption process of the selected folder. To do this, press **Options** → **Encrypt**.

   To move around the file system use the device's stylus or joystick buttons, as follows: **Up** and **Down** – to move within the selected folder, **Left** and **Right** – to move one level up or down from the current folder.

4. Press **OK**.

   The encrypted folder is added to the folders list.

In the **Options** menu for the encrypted folder, the menu item **Encrypt** changes to **Decrypt**.

After the encryption process, the data are automatically decrypted and encrypted when you work with data from the encrypted folder, move them out of the encrypted folder or place new data in the latter.

To encrypt all folders from the list at the same time, perform the following steps:

1. Select the **Folders list** item on the **Encryption** tab.

   This will open the **Folders list** window.

2. Select **Options** → **Add. actions** → **Encrypt all**.

3. Press **OK**.

DATA DECRYPTION

You can decrypt previously encrypted data (see "Data encryption" section on page 103). You can decrypt one or all encrypted folders on the device.

To decrypt a previously encrypted folder:

1. On the **Encryption** tab, select the **Folders list**.

   The **Folders list** window will open, which contains a list of all previously decrypted and encrypted folders.

2. Select the folder from the list which you wish to decrypt and then select **Options** → **Decrypt** (see figure below).

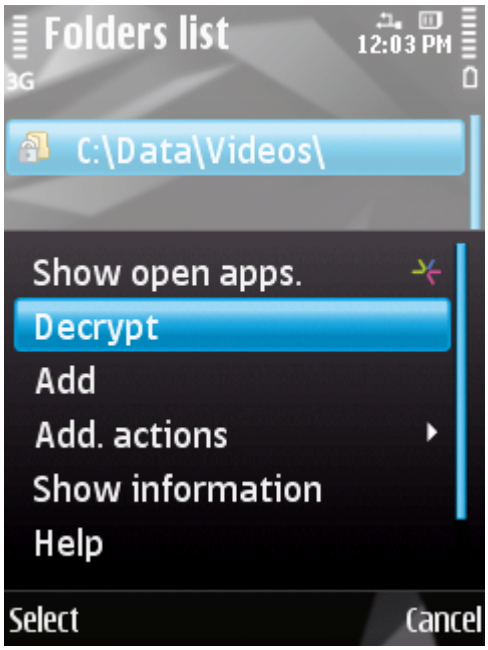


Figure 55: Data decryption

3. Press **OK** on completion of the data decryption.

When the decryption process is finished, the name of the **Decrypt** item is changed to **Encrypt** in the **Options** menu. You can use data encryption again (see "Data encryption" section on page 103).

To decrypt all folders from the list at the same time, perform the following steps:

1. On the **Encryption** tab, select the **Folders list**.

   This will open the **Folders list** window.

2. Select **Options** → **Add. actions** → **Decrypt all**.

3. Press **OK**.

BLOCKING ACCESS TO ENCRYPTED DATA

Encryption can set the time by when blocking access to encrypted folders starts. This functionality is activated when your device goes to power save mode. To manipulate encrypted data, enter the application PIN code.

In addition, you can immediately block access to encrypted folders after opening them, and enable the prompt for the application secret code.

To block access to an encrypted folder during this time:

1. Select the **Encryption** tab, select the **Block access** item.

   This will open the **Block access** window.

2. Enter the time after which the device switches to idle mode in which the data are accessible. To do this, select one of the suggested values (see Figure below):

   - **No delay**.
   - **After 1 minute**.
   - **After 5 minutes**.
   - **After 15 minutes**.
   - **After 1 hour**.

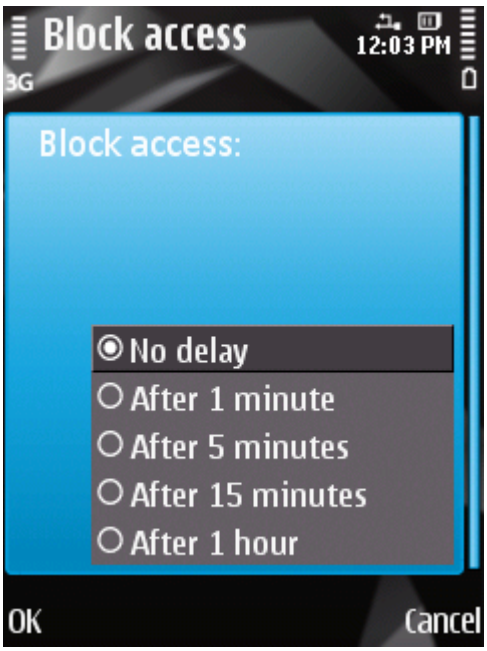


Figure 56: Blocking access to encrypted data

3. Press **OK** to save the changes.

To block access to the encrypted data and enable the secret code prompt at once,

press the"0" and "1" buttons on the device simultaneously.

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

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.

The Internet connection settings are established automatically by default. If the Internet connection settings are not established automatically, configure them (see the “Configuring Internet connection settings” section on page 110).

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 updating Kaspersky Mobile Security 9 anti-virus databases in order to avoid unnecessary costs.

The database issue date can be seen in the protection status window (see the “Protection status window” section on page 43). Details information on the anti-virus databases used is available on the **Additional** tab in the **Database info** menu item.

Information about anti-virus database updates is recorded in the application's log (see the "Application logs" section on page 112).

VIEWING DATABASE INFORMATION

You can view the following information about the application's installed anti-virus databases: last update, date of release of the database, database size and number of entries in them.

- *To view information about the current anti-virus databases,*

  on the **Additional** tab, select **Database info**.

STARTING UPDATES MANUALLY

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

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

  1. Select the **Update** item on the **Anti-Virus** tab.

     This will open the **Update** window.

  2. Select the **Update** item (see Figure below).

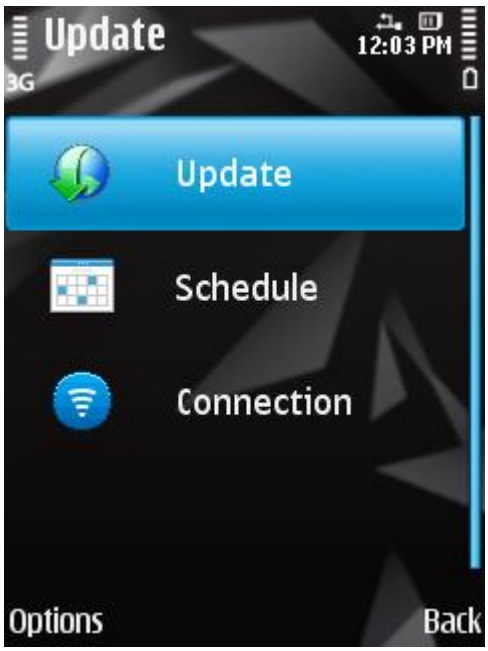


Figure 57: Starting the update manually

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 configure automatic update settings for when you are in a roaming zone (see the “Updating in roaming” section on page 110).

To configure a scheduled update start:

1. Select the **Update** item in the **Anti-Virus** tab.

   This will open the **Update** window.

2. Select the **Schedule** item.

   This will open the **Schedule** screen.

3. Set for the **Auto update** setting one of the values suggested (see Figure below):

   - **Off**: do not update the application database per schedule.
   - **Weekly**: perform the update once a week. Select the values for the **Update day** and **Update time**.
   - **Daily**: update application database every day. Enter the value for the **Update time**.

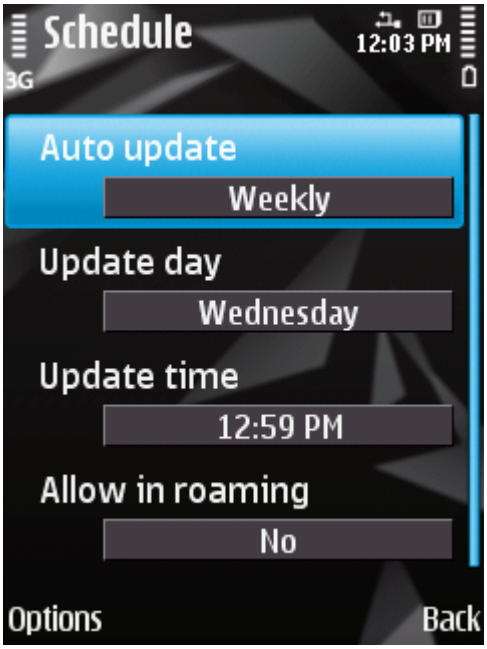


Figure 58: Configuration of automatic update on schedule

4. Press **Back** to save the changes.

UPDATING WHILE ROAMING

You can control the start of a scheduled update when the device is in a roaming zone, as Internet activity will be priced at roaming rates.

If the start of a scheduled update is blocked in roaming, manual updating will still be available in regular mode.

To disable scheduled anti-virus database updates when in a roaming zone, perform the following steps:

1. Select the **Update** item on the **Anti-Virus** tab.

   This will open the **Update** window.

2. Select the **Schedule** item.

   This will open the **Schedule** screen.

3. Select for the **Allow in roaming** setting the value **No** (see Figure below).

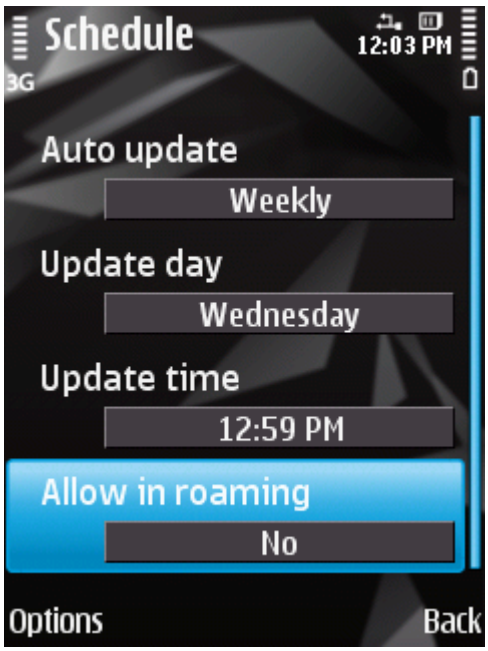


Figure 59: Configuring updates in roaming

4. Press **Back** to save the changes.

CONFIGURATION OF INTERNET CONNECTION SETTINGS

For connection to the Internet Kaspersky Mobile Security 9 uses an access point which is set by default.

The access points settings are issued by the provider.

If Kaspersky Mobile Security 9 has not specified the connection settings automatically, configure them.

To configure the Internet connection settings, perform the following steps:

1. Select the **Update** item on the **Anti-Virus** tab.

This will open the **Update** window.

2. Select the **Connection** item.

3. Select the access point which will be used to connect to the update server. To do this, select a value for the **Access point** setting and then press **OK** (see Figure below).

   The list shows all access points set on the mobile device.

Figure 60: Internet connection settings

4. Press **Back** to save the changes.

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).

IN THIS SECTION

ABOUT LOGS

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

For every component, a separate events log is used.

VIEWING LOG RECORDS

To view entries in the component's log, perform the following steps:

1. On the tab of any component, select the **Log**.

   A log of the component selected opens (see Figure below).

Figure 61: Selected component log

2. Use the joystick buttons or the stylus to navigate through the journal: **up** and **down** – view events in the current log, **left** and **right** - view events in the logs of other components.

To view detailed log record information,

select the necessary entry and then select **Options** → **Show information**.

DELETING LOG RECORDS

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

To delete all entries from the log, perform the following steps:

1. On the tab of any component, select the **Log**.

   This will open the **Log** window.

2. Select **Options** → **Clear Log**.

All records from all component logs will be deleted.

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.

IN THIS SECTION

CHANGING THE SECRET CODE

You can change the secret code of the application set after the activation.

To change the secret code:

1. On the **Additional** tab, select the **Settings** item.

   This will open the **Settings** window.

2. Select the **Change code** setting.

3. Enter the current code in the **Enter code** field and press **OK**.

4. Enter a new code in the **Enter new code** field and press **OK**.

5. Enter the code again in the **Confirm code** field and press **OK**.

DISPLAYING HINTS

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

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

1. Select the **Settings** item on the **Additional** tab.

   This will open the **Settings** window.

2. Select one of the values suggested for the **Hints** setting:

   - **Show**: display hints before configuring the settings of the function selected.

- **Hide**: do not display hints.

3. Press **Back** to save the changes.

CONFIGURING SOUND NOTIFICATIONS

As a result of the application's operation, specific events occur: for instance an infected object or virus is found, the license term is coming to an end. 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 edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

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

1. On the **Additional** tab, select the **Settings** item.

   This will open the **Settings** window.

2. Select one of the values suggested for the **Sound notifications** setting:

   - **Always**: notify with sound regardless of the device's selected profile.
   - **According to profile**: use the sound notification depending on the selected device mode.
   - **Disable**: do not use sound notification.

3. Press **OK** to save the changes.

MANAGING THE BACKLIGHT

When the application performs protection tasks, high levels of power are consumed. To save power while executing these tasks, the application allows disabling the screen backlight automatically.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To configure the screen backlight while executing tasks, perform the following steps:

1. Select the **Settings** item on the **Additional** tab.

   This will open the **Settings** window.

2. Select one of the values suggested for the **Backlight** setting (see Figure below):

   - **According to profile**: use the screen backlight depending on the selected device mode.

- **Enable**: always use the screen backlight.

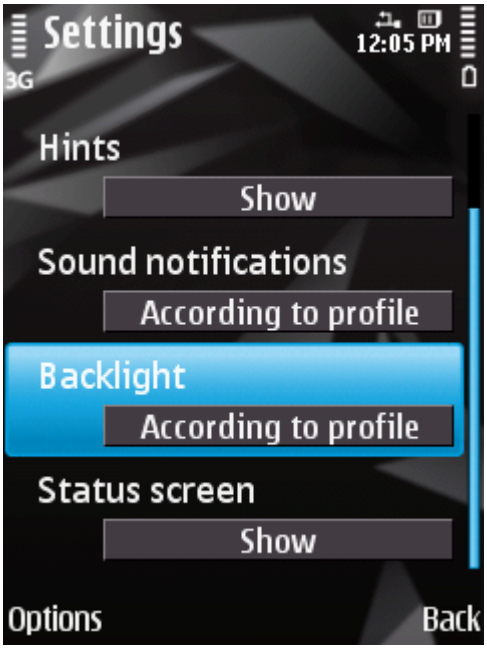


Figure 62: Managing the backlight

3. Press **Back** to save the changes.

DISPLAYING THE STATUS WINDOW

You can choose whether or not to display the application's status window when the application starts.

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To configure the status window display when starting the application, perform the following steps:

1. Select the **Settings** item on the **Additional** tab.

   This will open the **Settings** window.

2. Select one of the values suggested for the **Status screen** (see Figure below):

   - **Show**: show status window.

- **Hide**: do not show status window.

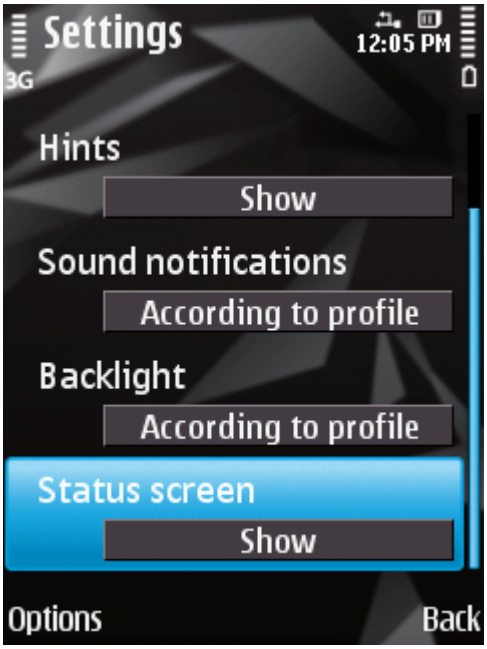


Figure 63: Configuring the status window display

3. Press **Back** to save the changes.

DISPLAYING THE PROTECTION ICON

To see the Protection status, you can configure the display of the protection icon on the mobile device's screen (see “Protection icon section” on page 43).

To edit the settings, use the device's joystick or stylus, or select **Options** → **Change**.

To change the display settings of the protection icon, perform the following steps:

1. Select the **Protection** item in the **Anti-Virus** tab.

   This will open the **Protection** window.

2. Select one of the suggested values for the **Protection icon** setting (see Figure below):

   - **Always show**: show the protection icon on the device's screen.
   - **In menu only**: show the protection icon only when the device menu or the Kaspersky Mobile Security 9 menu is open.

- **Do not show**: do not show the protection icon.

Figure 64: Protection icon display settings

3. Press **OK** to save the changes.

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

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.

BLOCKING AN OBJECT

Denying access to an object from external applications. A blocked object cannot be read, executed, modified or deleted.

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

DISINFECTING OBJECTS

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.

F

FILE MASK

Representation of a file name and extension using wildcards. The two basic wildcards used in file masks are "*" and "?", where "*" represents any number of any characters and "?" stands for any single character. Using these wildcards, you can represent any file. Note that the file name and file extension are always separated by a period.

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.

L

LICENSE PERIOD

Period of time during which you are able to use all of the features of your Kaspersky Lab application. When the license expires, the application switches to limited functionality mode. In this mode, the following actions are available in the application:

- disabling all components;
- encryption of one or several folders;
- disabling hiding of personal data;
- blocking automatic hiding confidential information;
- viewing application's help system.

N

NON-NUMERIC NUMBER

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

O

ON-DEMAND SCANS

An operation mode of the Kaspersky Lab application, which is initiated by the user and intended for scanning of any files.

P

PLACING OBJECTS INTO QUARANTINE

A method used to process a possibly infected object, by blocking access to the object and moving it from its original location to the Quarantine folder. In Quarantine the object is stored in encrypted form, which prevents it from infecting the device.

Q

QUARANTINE

The folder created to store all possibly infected objects detected by device scans or through the process of Protection.

R

RESTORING AN OBJECT

Moving an object from Quarantine to its original folder (where it had been stored before it was quarantined, disinfected, or deleted), or to another user-defined folder.

U

UPDATING DATABASES

One of the functions that Kaspersky Lab application performs which keeps protection up to date. Anti-virus databases are copied from Kaspersky Lab update servers onto the device and the application is automatically connected to them.

W

WHITE LIST

The entries in this list contain the following information:

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

KASPERSKY LAB

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

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

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

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

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

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

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

Kaspersky Lab website	http://www.kaspersky.com
Virus Encyclopedia:	http://www.securelist.com/
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending suspicious objects in archives) http://support.kaspersky.com/virlab/helpdesk.html (for sending requests to virus analysts)
Kaspersky Lab web forum:	http://forum.kaspersky.com

INFORMATION ABOUT THIRD PARTY CODE

Third party code is used to create the application.

IN THIS SECTION

DISTRIBUTED PROGRAM CODE

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

IN THIS SECTION

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

B

C

D

E

F

I

L

M

N

O

P

Q

R

S

U

W