

Kaspersky Endpoint Security 8 for Smartphone

for BlackBerry OS

The Kaspersky logo is displayed in a large, bold, teal font, slanted upwards from left to right. The word "KASPERSKY" is in teal, and the word "lab" is in red. The logo is positioned on a white diagonal band that cuts across the teal background.

User guide

PROGRAM VERSION: 8.0

Dear User!

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

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

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

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

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

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

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

Revision date: 20.10.2010

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved.

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

KASPERSKY LAB END USER LICENSE AGREEMENT

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

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

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER CURRENT END USER LICENSE AGREEMENT.

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. You are given 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 *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.
- 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.
- 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.
- 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.
- 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 (30 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.
- 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 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.

4. Technical Support

- 4.1. 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>

- 4.2. User's Data, specified in Personal Cabinet/My Kaspersky Account, can be used by Technical Support specialists only during processing User's request.

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.

- 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.
- 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. Your key file can be blocked in case You breach any of the terms and conditions of this Agreement.
- 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. 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.
- 6.4. 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.
- 6.5. 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.
- 6.6. 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

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

WARRANTY OF THE Rightholder AND/OR ANY OF ITS PARTNERS, EVEN IF THE Rightholder AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

8. GNU and Other Third Party Licenses

- 8.1. 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 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

- 10.1. 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

11.1. 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

12.1. 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

© 1997-2010 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

TABLE OF CONTENTS

KASPERSKY LAB END USER LICENSE AGREEMENT	3
ABOUT THIS HELP	10
ADDITIONAL DATA SOURCES	11
Information sources for further research.....	11
Discussion of Kaspersky Lab applications on the Web forum	12
Contacting the Documentation Development Group	12
KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE	13
HARDWARE AND SOFTWARE REQUIREMENTS.....	13
INSTALLING KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE	13
About installing the application through the computer	14
Installing the application through the computer	14
About installing the application after receiving a message by email	16
Installing the application after receiving a message by email	16
MANAGING APPLICATION SETTINGS	17
UNINSTALLING THE APPLICATION	18
MANAGING THE LICENSE	18
About Kaspersky Endpoint Security 8 for Smartphone licenses	19
Installing a license	20
Viewing license information	20
SYNCHRONIZING THE DEVICE WITH THE REMOTE ADMINISTRATION SYSTEM.....	20
Start synchronization manually.....	21
Changing the synchronization settings	21
GETTING STARTED.....	22
Starting the application	22
Entering the secret code.....	23
Viewing information about the application	23
APPLICATION INTERFACE	23
Application menu	24
Protection status window	24
FILTERING OF INCOMING CALLS AND SMS.....	25
About Anti-Spam	25
Anti-Spam modes.....	26
Changing the Anti-Spam mode.....	26
Creating a Black List.....	27
Adding entries to the Black List.....	27
Editing entries in the Black List	28
Deleting entries from the Black List.....	29
Creating a White List	29
Adding entries to the White List	30
Editing entries in the White List.....	31
Deleting entries from the White List	32

Responding to SMS messages and calls from contacts not in the phone book.....	32
Responding to SMS messages from non-numeric numbers.....	33
Selecting a response to incoming SMS	34
Selecting a response to incoming calls.....	35
DATA PROTECTION IN THE EVENT OF LOSS OR THEFT OF THE DEVICE.....	35
About Anti-Theft.....	36
Blocking the device.....	36
Deleting personal data.....	38
Creating a list of folders to delete	39
Monitoring the replacement of a SIM card on the device.....	40
Determining the device's geographical coordinates.....	41
Remote start of the Anti-Theft functions	43
PRIVACY PROTECTION.....	44
Privacy Protection.....	44
Privacy Protection modes	44
Enabling/disabling Privacy Protection.....	45
Enabling Privacy Protection automatically	45
Enabling Privacy Protection remotely	46
Selecting data to hide: Privacy Protection	48
Creating a list of private numbers	48
Adding a number to the list of private numbers.....	49
Editing a number in the list of private numbers	49
Deleting a number from the list of private numbers.....	50
APPLICATION LOGS.....	50
About logs.....	51
Viewing Log records	51
Deleting Log records	51
CONFIGURING ADDITIONAL SETTINGS	51
Changing the secret code.....	52
Displaying prompts	52
GLOSSARY	53
KASPERSKY LAB.....	55
USING THIRD-PARTY CODE	56
INDEX	57

ABOUT THIS HELP

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

Objectives of the document:

- help the 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.

ADDITIONAL DATA SOURCES

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

IN THIS SECTION

Information sources for further research	11
Discussion of Kaspersky Lab applications on the Web forum	12
Contacting the Documentation Development Group	12

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;
- the installed application documentation.

Page on Kaspersky Lab website

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

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

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

<http://support.kaspersky.com/kes8mobile>

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

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

The installed Help system

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

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

The installed Documentation

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

DISCUSSION OF KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

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

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

CONTACTING THE DOCUMENTATION DEVELOPMENT GROUP

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

KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

Kaspersky Endpoint Security 8 for Smartphone protects mobile devices working on BlackBerry OS. The application controls incoming SMS and calls, protects information on the device in case of theft or loss, and hides information relating to confidential contacts. Every type of threat is processed in separate components of the program. This allows to fine-tune the application settings depending on user needs. The administrator installs the application and configures and updates settings using the remote administration system.

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

- **Anti-Spam.** Scans all incoming SMS messages and calls for spam. The component allows the flexible blocking of text messages and calls considered undesirable.
- **Anti-Theft folder.** This protects information on the device from unauthorized access when it is lost or stolen and also makes it easier to find. Anti-Theft enables you to lock your device remotely, delete any information stored there, and pinpoint its geographic location (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.
- **Privacy Protection.** It hides information related to confidential numbers from the contact list. For these numbers, Privacy Protection hides entries in Contacts and in the Incoming and Outgoing Calls Register.

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

- **Protection status.** The status of the program's components is displayed on screen. Based on the information presented, you can evaluate the current information protection status on your device.
- **Events log.** Each of the program's components has its own events log, which contains information about the component's operations (e.g. remote launch of the Anti-Theft function, status of the program's license validity period). Reports on the operation of components are given in the remote administration system and remain in it.
- **Uninstalling the application.** To prevent access to protected information, Kaspersky Endpoint Security 8 for Smartphone can only be uninstalled from the application's interface.

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

HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Endpoint Security 8 for Smartphone can be installed on mobile devices using the BlackBerry OS 4.5, 4.6, 4.7, 5.0 and 6.0 operating systems.

INSTALLING KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE

The administrator installs Kaspersky Endpoint Security 8 for Smartphone using remote administration. Installing the application requires additional action from the user.

The application is installed by following one of the following procedures:

- The Kaspersky Endpoint Security 8 for Smartphone application installation utility of the same name is installed on your computer. With its help, you can install Kaspersky Endpoint Security 8 for Smartphone on your mobile device.
- A message from the administrator with the distribution package or an indication to download it comes to your email address. You install Kaspersky Endpoint Security 8 for Smartphone on your mobile device using information from the message.

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

IN THIS SECTION

About installing the application through the computer [14](#)

Installing the application through the computer [14](#)

About installing the application after receiving a message by email..... [16](#)

Installing the application after receiving a message by email..... [16](#)

ABOUT INSTALLING THE APPLICATION THROUGH THE COMPUTER

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

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

INSTALLING THE APPLICATION THROUGH THE COMPUTER

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

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

➔ *To install the application on a mobile device through a workstation, perform the following:*

1. Connect the mobile device to the workstation using Blackberry Desktop Manager.

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



Figure 1: Installer for Kaspersky Endpoint Security 8 for Smartphone

2. Click the **Continue** button.

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

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

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

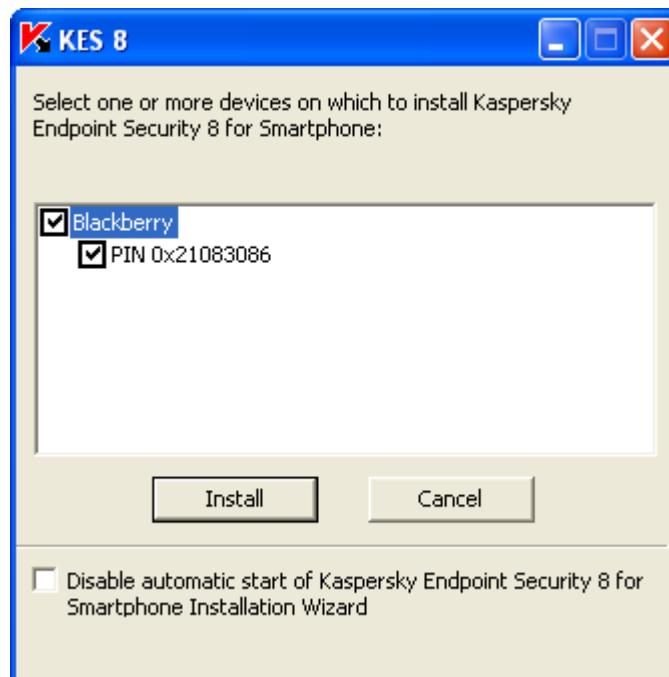


Figure 2: Selecting devices for installation of Kaspersky Endpoint Security 8 for Smartphone

4. Press **Install** button.

The **Application Download Wizard** window opens on the computer. After the distribution package is transferred onto the chosen devices, application installation starts automatically. After the installation has completed, press **Close** on the **Application Download Wizard** window.

The status of transmitting the application distribution package to the device is also displayed on the computer in the **Kaspersky Endpoint Security 8 for Smartphone** window.

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

➔ To stop Kaspersky Endpoint Security 8 for Smartphone being installed on subsequent connections of the devices to the computer,

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

ABOUT INSTALLING THE APPLICATION AFTER RECEIVING A MESSAGE BY EMAIL

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

The message contains the following information:

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

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

INSTALLING THE APPLICATION AFTER RECEIVING A MESSAGE BY EMAIL

If you have received an email message with application settings, you can only install the application through the mobile device itself. In this case, installation of Kaspersky Endpoint Security 8 for Smartphone through a computer is not supported.

➔ To install Kaspersky Endpoint Security 8 for Smartphone:

1. Open the message containing the application's installation settings from the administrator on the mobile device.
2. Perform one of the following actions:
 - if the message has a link, follow it to download the distribution package;
 - if the distribution package is in an attachment to the message, download the distribution package.

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

3. Run the application (see "Starting the application" on page [22](#)). To do this, select **Menu** → **Download** → **KES 8** and launch the application by using the scroll bar or selecting **Menu** → **Open**.
4. Set the application secret code (see "Entering the secret code" on page [23](#)). To this end, fill in the **Enter new code** and **Confirm code** fields and press **ENTER**.

This will open **Synchronization settings** window.

Figure 3: Synchronization settings

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

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

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

6. In the **Your email address** field, enter your business email address and press **OK**.

Enter the email address correctly since it is used to register the device on the remote administration system.

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

MANAGING APPLICATION SETTINGS

All the operation settings for Kaspersky Endpoint Security 8 for Smartphone, including the license, are configured by the administrator through the remote administration system. The administrator can then allow or block the user changing the values of these settings.

You can change the operating settings of the application on your mobile device if the administrator has not blocked the changing of these parameters.

If the component settings screen has a lock icon and a warning message at the top, the component settings cannot be accessed to be changed on the mobile device.

If the administrator changed the application settings, they will be transferred to the device through the remote administration system. In this case the values of the application settings which the administrator has blocked will change. Settings which the administrator has not blocked remain unchanged with the values that were configured earlier.

If the application settings were not received on the device or if you want to configure the values set by the administrator, use synchronization of the device with the remote administration system (see "Start synchronization manually" on page [21](#)).

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

UNINSTALLING THE APPLICATION

The application can only be uninstalled from the device manually by the user.

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

➤ *To uninstall Kaspersky Endpoint Security 8 for Smartphone manually:*

1. Disable hiding of confidential information (see section "Enabling/disabling Privacy Protection" on page [45](#)).
2. Uninstall Kaspersky Endpoint Security 8 for Smartphone To do this, select **Delete application** on the **Additional** tab (see Figure below).

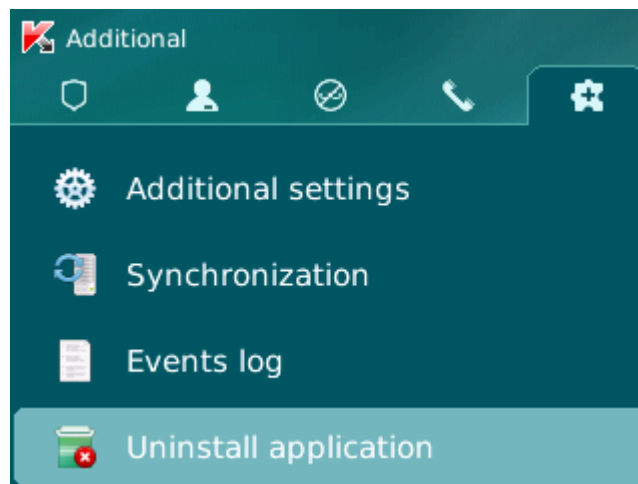


Figure 4: Uninstalling the application

A confirm deletion window opens.

3. Confirm the deletion of Kaspersky Endpoint Security 8 for Smartphone by clicking **Yes**.

The deletion of the application begins.

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

MANAGING THE LICENSE

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

IN THIS SECTION

About Kaspersky Endpoint Security 8 for Smartphone licenses.....	19
Installing a license.....	20
Viewing license information.....	20

ABOUT KASPERSKY ENDPOINT SECURITY 8 FOR SMARTPHONE LICENSES

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

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

Every license has a validity period and type.

The *license validity period* is the period for which you are provided with technical support.

The scope of services provided depends on the license type.

The following license types are available:

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

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

- disabling the Privacy Protection component;
- viewing application's help system;
- synchronization with the remote administration system.
- *Commercial* – paid license with a limited validity period (for example, one year), provided upon purchase of Kaspersky Endpoint Security 8 for Smartphone.

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

On termination of the commercial license's term of validity, Kaspersky Endpoint Security 8 for Smartphone switches to the limited functionality mode. The following are accessible in this mode:

- disabling the Anti-Theft and Privacy Protection components;
- disabling hiding of personal data;
- viewing application's help system;
- synchronization with the remote administration system.

INSTALLING A LICENSE

The administrator installs the license through the remote administration system.

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

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

- disabling all components;
- disabling hiding confidential data;
- viewing application's help system.

If the license was not installed within three days, install it using synchronization of the device with the remote administration system (see "Start synchronization manually" on page [21](#)).

VIEWING LICENSE INFORMATION

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

➔ *To view the license information:*

1. Open the **Additional** tab.
2. Select **About license**.

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

SYNCHRONIZING THE DEVICE WITH THE REMOTE ADMINISTRATION SYSTEM

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

The device is automatically synchronized with the remote administration system.

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

Manual synchronization is required in the following situations:

- if the license was not installed within three days of the application being installed;
- if the application settings given by the administrator were not received by the device.

According to the remote administration system chosen by the administrator to manage the application, the user may be asked to enter connection settings to the remote administration system. In this case, the values set by the user manually are accessible for changes from the application (see "Changing the synchronization settings" on page [21](#)).

START SYNCHRONIZATION MANUALLY

➤ To manually synchronize the device with the remote administration system:

1. Open the **Additional** tab.
2. Select the **Synchronization** item (see Figure below).

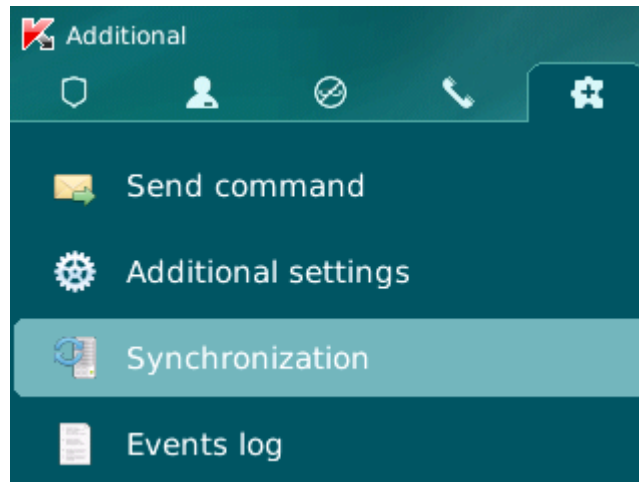


Figure 5: Manual synchronization

If the user was not asked to enter the settings for connection to the remote administration system when installing the application, a window appears with confirmation of the Internet connection setting. Allow connection by clicking on **Yes**. Internet connection with the remote administration system will be set.

If the user was asked to enter settings for connection to the remote administration system when installing the application, the **Synchronization** screen opens. Select **Start synchronization**. Allow connection to the Internet by clicking on **Yes**. Internet connection with the remote administration system will be set.

CHANGING THE SYNCHRONIZATION SETTINGS

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

➤ To change settings for connection to the remote administration:

1. Open the **Additional** tab.
2. Select **Synchronization**.
This will open the **Synchronization** window.
3. Select **Synchronization settings**.
4. Change the following settings (see Figure below):
 - **Server**;
 - **Port**;
 - **Group**.

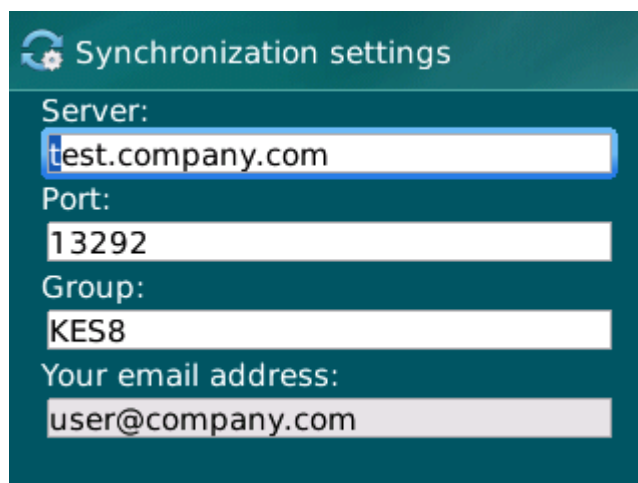


Figure 6: Changing the synchronization settings

5. Select **Menu** → **Save**.

GETTING STARTED

This section contains information about getting started with Kaspersky Endpoint Security 8 for Smartphone: how to set a secret code for the application, start the application and view information about it.

IN THIS SECTION

Starting the application.....	22
Entering the secret code	23
Viewing information about the application	23

STARTING THE APPLICATION

➔ To start Kaspersky Endpoint Security 8 for Smartphone:

1. Open the device's main menu.
2. Select the folder **Download** → **KMS 8**.

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

3. Start the application. To do this, use the scroll bar or select **Menu** → **Open**.
4. Enter the application secret code (see Section "Entering the secret code" on page [23](#)) and press **ENTER** on the keyboard.

A window opens showing the protection status of Kaspersky Endpoint Security 8 for Smartphone (see the "Protection status window" on page [24](#)).

ENTERING THE SECRET CODE

After launching the application, you will be prompted to enter a secret code. The *secret code* prevents unauthorized access to the application settings. You can later change the secret code installed.

The secret code is requested in the following instances:

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

Keep the secret code in mind. If you forget it, you will not be able to manage the functions of Kaspersky Endpoint Security 8 for Smartphone or uninstall the application.

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

➤ *To enter the secret code:*

1. Confirm that you wish to create an application secret code. To do this, after the application first launches, press **OK** in the Notifications window.

The screen for entering the application secret code opens.

2. Enter the figures that will form your code in the **Enter new code** field.
3. Re-enter the same code in the **Confirm code** field.
4. Press **ENTER** on the keyboard.

The code entered is automatically verified.

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

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

To make a new code, press **No** button. The **Enter new code** and **Confirm code** fields will empty. Enter a new application secret code.

VIEWING INFORMATION ABOUT THE APPLICATION

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

➤ *To view information on the application,*

select the **Additional**, select **About**.

APPLICATION INTERFACE

The Kaspersky Endpoint Security 8 for Smartphone interface is simple and convenient. This section provides information on its main elements.

IN THIS SECTION

Application menu..... [24](#)
 Protection status window..... [24](#)

APPLICATION MENU

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

The Kaspersky Endpoint Security 8 for Smartphone menu contains the following tabs:

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

You can switch between tabs by using the scroll bar.

PROTECTION STATUS WINDOW

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

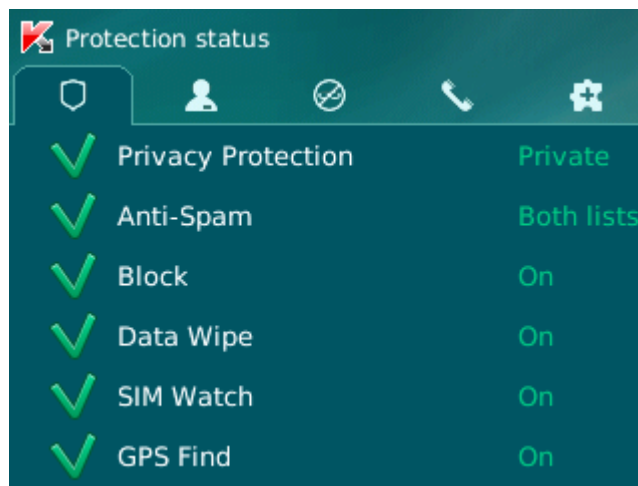


Figure 7: Current status window

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

- **Privacy Protection** is the status of hiding confidential information (see "Hiding confidential information" on page [44](#)).

The **Normal** status means that hiding of confidential information is disabled. The **Private** status means that hiding of confidential information is enabled.

- **Anti-Spam** is the SMS and call filtering mode (see "Filtering of incoming calls and SMS" on page [25](#)).
- **Block, Data Wipe, SIM Watch, GPS Find** represent the Anti-Theft status (see Section "Data protection in the event of loss or theft of the device" on page [35](#)).

The **Enabled** status means that the Anti-Theft function is enabled. The **Disabled** status means that the **Anti-Theft** function is disabled.

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

FILTERING OF INCOMING CALLS AND SMS

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

IN THIS SECTION

About Anti-Spam	25
Anti-Spam modes.....	26
Changing the Anti-Spam mode	26
Creating a Black List	27
Creating a White List.....	29
Responding to SMS messages and calls from contacts not in the phone book	32
Responding to SMS from non-numeric numbers	33
Selecting a response to incoming SMS.....	34
Selecting a response to incoming calls	35

ABOUT ANTI-SPAM

Anti-Spam blocks unwanted calls and messages based on a White and a Black list you compile.

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

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

Anti-Spam filters incoming messages and calls according to the chosen mode (see "Anti-Spam modes" on page 26). According to the mode, Anti-Spam scans every incoming SMS or call and then determines whether this SMS or call is wanted or unwanted (spam). As soon as Anti-Spam assigns the wanted or unwanted status to an SMS or call, the scan is finished.

Information about blocked SMS and calls is registered in the application's log (see section "Application logs" on page 50).

ANTI-SPAM MODES

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

The following Anti-Spam modes are available:

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

You can change the Anti-Spam mode (see the "Changing the Anti-Spam mode" section on page 26). The current Anti-Spam mode is displayed in the **Anti-Spam** tab next to the **Mode** menu item.

CHANGING THE ANTI-SPAM MODE

➔ To select an Anti-Spam operation mode:

1. Select the **Mode** item in the **Anti-Spam** tab.

This will open the **Anti-Spam** window.

2. Select a value for the **Anti-Spam mode** setting (see Figure below).

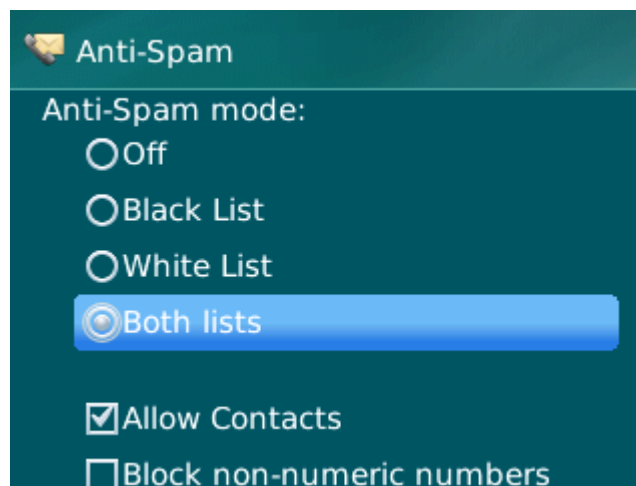


Figure 8: Changing the Anti-Spam mode

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

CREATING A BLACK LIST

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

- Phone number from which Anti-Spam blocks calls and / or SMS.
- Types of events from this number that Anti-Spam blocks. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase that Anti-Spam uses to classify an SMS as unsolicited (spam). Anti-Spam only blocks SMS that contain this key phrase, while delivering all other ones.

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

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

Information about blocked SMS and calls is registered in the log (see the "Application logs" section on page [50](#)).

IN THIS SECTION

Adding entries to the Black List	27
Editing entries in the Black List	28
Deleting entries from the Black List.....	29

ADDING ENTRIES TO THE BLACK LIST

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

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

1. Select **Black List** in the **Anti-Spam** tab.
This will open the **Black List** window.
2. Select **Menu** → **Add**.
This will open the **New entry** window.
3. Set values for the following settings (see Figure below):
 - **Block incoming** – type of event from a telephone number which Anti-Spam blocks for Black List numbers:
 - **Calls and SMS**: block incoming calls and SMS messages.
 - **Calls only**: block incoming calls only.
 - **SMS only**: block incoming SMS messages only.

- **Phone number** – telephone number for which Anti-Spam blocks incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+" symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any amount of symbols, and "?" any one symbol). For example, *1234? on the Black List. Anti-Spam 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). Anti-Spam only blocks those messages that have the key phrase, it allows all other SMS messages.

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.

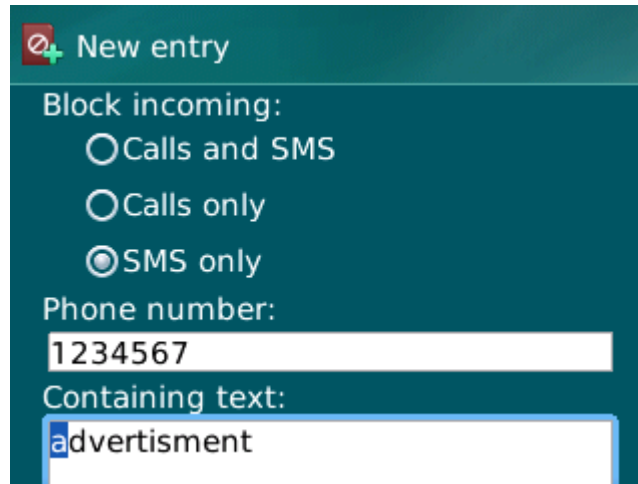


Figure 9: Properties of an entry on the Black List

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

EDITING ENTRIES IN THE BLACK LIST

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

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

1. Select **Black List** in the **Anti-Spam** tab.

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

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

The **Changing an entry** screen opens.

3. Change the necessary settings:

- **Block incoming** – type of event from a telephone number which Anti-Spam blocks for Black List numbers:
 - **Calls and SMS**: block incoming calls and SMS messages.
 - **Calls only**: block incoming calls only.
 - **SMS only**: block incoming SMS messages only.
- **Phone number** – telephone number for which Anti-Spam blocks incoming information. The phone number should comprise only alphanumeric characters; it may begin with a digit, a letter, or be preceded by the "+"

symbol. As a number, it is also possible to use the masks "*" or "?" (where "*" is any amount of symbols, and "?" any one symbol). For example, *1234? on the Black List. Anti-Spam 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). Anti-Spam only blocks those messages that have the key phrase, it allows all other SMS messages.

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

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

DELETING ENTRIES FROM THE BLACK LIST

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

➤ *To delete an entry from the Parental Control Black List:*

1. Select **Black List** in the **Anti-Spam** tab.
This will open the **Black List** window.
2. Select the entry to be deleted on the list and then select **Menu** → **Delete**.
The confirmation window opens.
3. Confirm the deletion by pressing the **Yes** button.

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

1. Select **Black List** in the **Anti-Spam** tab.
This will open the **Black List** window.
2. Select **Menu** → **Delete all**.
The confirmation window opens.
3. Confirm the deletion by pressing the **Yes** button.

The list is emptied.

CREATING A WHITE LIST

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

- Phone number from which Anti-Spam delivers calls and / or SMS.
- Type of events that Anti-Spam delivers from this number. The following types of events are available: calls and SMS, calls only, and SMS only.
- Key phrase used by Anti-Spam to classify an SMS as solicited (not spam). Anti-Spam only delivers SMS that contain this key phrase, while blocking all other ones.

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

IN THIS SECTION

Adding entries to the White List..... [30](#)

Editing entries in the White List [31](#)

Deleting entries from the White List [32](#)

ADDING ENTRIES TO THE WHITE LIST

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

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

1. On the **Anti-Spam** tab, select the **White List**.

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

2. Select the **Menu** → **Add**.

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

- **Allow incoming** – type of event from a telephone number which Anti-Spam allows for Black List numbers:
 - **Calls and SMS:** allow incoming calls and SMS messages.
 - **Calls only:** allow incoming calls only.
 - **SMS only:** allow incoming SMS messages only.
- **Phone number** – telephone number for which Anti-Spam allows 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. Anti-Spam 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, Anti-Spam only delivers SMS messages containing the key phrase and blocks all others.

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

Figure 10: Properties of an entry on the White List

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

EDITING ENTRIES IN THE WHITE LIST

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

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

1. On the **Anti-Spam** tab, select the **White List**.

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

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

The **Changing an entry** screen opens.

3. Change the necessary settings:

- **Allow incoming** – type of event from a telephone number which Anti-Spam allows for Black List numbers:
 - **Calls and SMS:** allow incoming calls and SMS messages.
 - **Calls only:** allow incoming calls only.
 - **SMS only:** allow incoming SMS messages only.
- **Phone number** – telephone number for which Anti-Spam allows 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. Anti-Spam 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, Anti-Spam only delivers SMS messages containing the key phrase and blocks all others.

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

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

DELETING ENTRIES FROM THE WHITE LIST

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

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

1. On the **Anti-Spam** tab, select the **White List**.

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

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

The confirmation window opens.

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

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

1. On the **Anti-Spam** tab, select the **White List**.

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

2. Press **Menu** → **Delete all**.

The confirmation window opens.

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

The White List is emptied.

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

If the **Both lists** or **White List** mode is selected for Anti-Spam (see section "**Anti-Spam modes**" on page [26](#)), you can also set an Anti-Spam response to SMS messages and calls from subscribers whose numbers are not stored in the Contacts. In addition, Anti-Spam allows expansion of the White List by adding numbers from the list of contacts to it.

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

1. Select the **Mode** item in the **Anti-Spam** tab.

This will open the **Anti-Spam** window.

2. Select the required value for setting **Allow Contacts** (see Figure below):

- for Anti-Spam to count numbers from Contacts as additional White List and block SMS messages and calls from subscribers not in Contacts, check the **Allow Contacts** box;
- to enable Anti-Spam to filter SMS messages and calls based on the Anti-Spam mode, uncheck the **Allow Contacts** box.

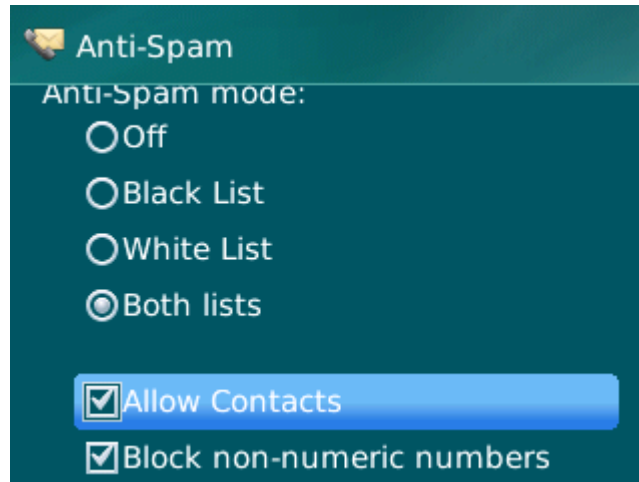


Figure 11: Anti-Spam response to numbers not included in the device's phone book

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

RESPONDING TO SMS MESSAGES FROM NON-NUMERIC NUMBERS

If the Anti-Spam mode **Both lists** or **Black List** is selected (see the "**Anti-Spam modes**" section on page [26](#)), you can also expand the Black List by including all non-numeric numbers (including letters). In this case, Anti-Spam processes calls and SMS messages from non-numeric numbers the same way as from numbers on the Black List.

➤ *To set Anti-Spam's response when receiving SMS messages from non-numeric numbers:*

1. Select the **Mode** item in the **Anti-Spam** tab.
2. This will open the **Anti-Spam** window.
3. Select a value for the **Block non-numeric numbers** setting (see Figure below):
 - in order for Anti-Spam to automatically block SMS from non-numeric numbers, check the **Block non-numeric numbers** box;
 - if you want Anti-Spam to filter SMS from non-numeric numbers on the basis of the Anti-Spam mode set, uncheck the **Block non-numeric numbers** box.

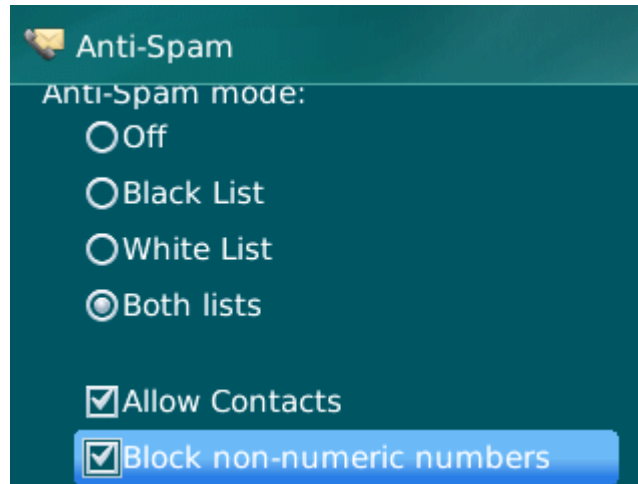


Figure 12: Selecting Anti-Spam action when receiving SMS from non-numeric numbers

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

SELECTING A RESPONSE TO INCOMING SMS

If the **Both lists** mode is set (see "Anti-Spam Modes" on page 26), Anti-Spam scans incoming SMS messages according to the Black and White Lists.

After receiving an SMS message from a number that is not included on either list, Anti-Spam will prompt you to enter the number in one of the lists.

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

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

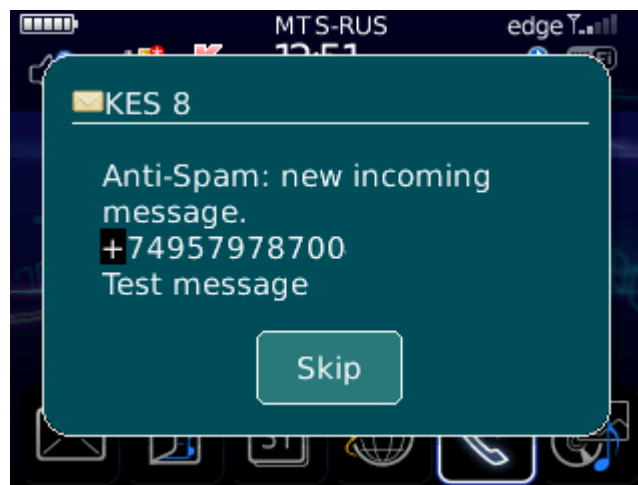


Figure 13: Anti-Spam notification on SMS received

Information about blocked SMS is registered in the application's log (see the "Application logs" section on page 50).

SELECTING A RESPONSE TO INCOMING CALLS

If **Both lists** mode is set (see "**Anti-Spam modes**" on page [26](#)), Anti-Spam checks incoming calls according to the Black and White Lists. Following a call from a number not on either list, Anti-Spam will prompt you to enter the number in one of the lists (see figure below).

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

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

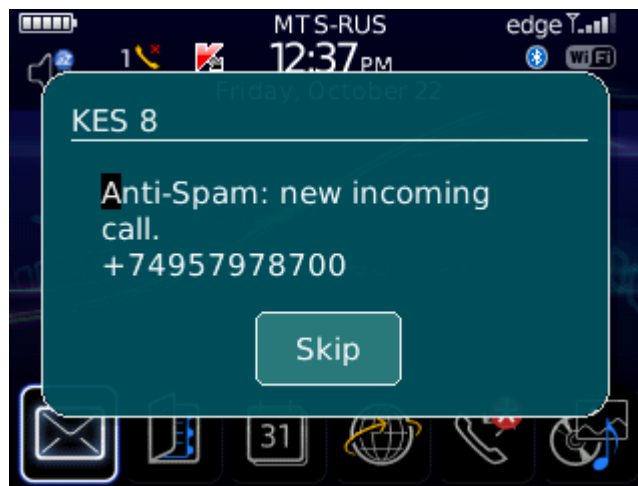


Figure 14: Anti-Spam notification on SMS received

Information about blocked calls is registered in the application's log (see the "Application logs" section on page [50](#)).

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 [36](#)

Blocking the device [36](#)

Deleting personal data [38](#)

Creating a list of folders to delete [39](#)

Monitoring the replacement of a SIM card on the device [40](#)

Determining the device's geographical coordinates [41](#)

Remote start of the Anti-Theft functions [43](#)

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** – allows deleting the user's personal data remotely from the device (entries in Contacts, messages, 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 have 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.

Kaspersky Endpoint Security 8 for Smartphone can start Anti-Theft remotely if you send an SMS command from another mobile device (see "Remote start of the Anti-Theft functions" on page [43](#)).

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

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

Information about the component's operation is entered in the application's log (see "Application Logs" on page [50](#)).

BLOCKING THE DEVICE

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

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

➤ *To enable the Block function:*

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

This will open the **Block** window.

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

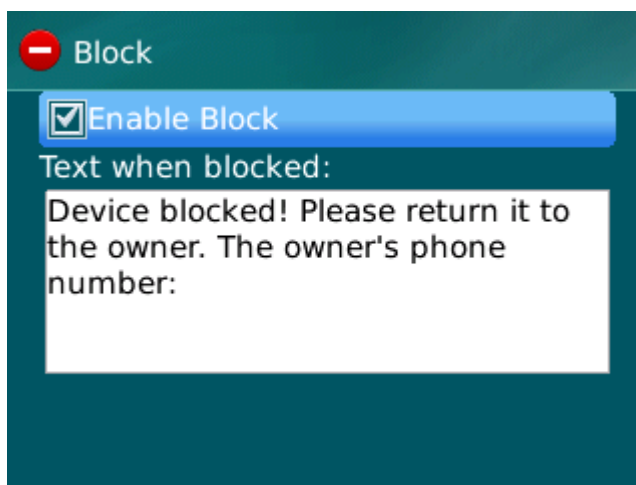


Figure 15: Block function settings

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

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

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

Outgoing SMS messages 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 Sending a command function:*

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

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

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

5. Select **Menu** → **Send**.

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

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

DELETING PERSONAL DATA

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

- the user's personal data (entries in Contacts, calendar, email messages, call log);
- information on storage card;
- files from the list of objects for deletion (see the "Creating a list of folders to delete" section on page [39](#)).

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

➤ To enable the Data Wipe function:

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

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

2. Select the **Mode** item.

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

3. Check the **Enable Data Wipe** box.

4. Select information that you want to delete. To do this, check the boxes next to the required settings in the **Delete** section (see Figure below).

- to delete personal data, check the **Personal data** box;
- to delete files from folders on the memory card and from the list of objects for deletion, check the box **Selected folders**.

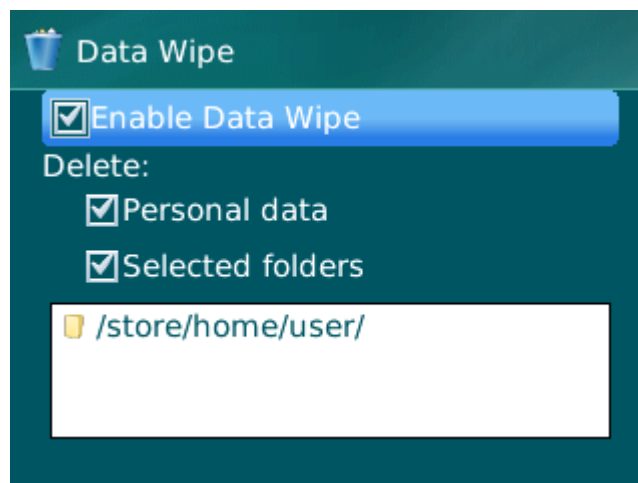


Figure 16: Data Wipe function settings

5. Go to creation of a list of objects for deletion (see the "Creating a list of folders to delete" section on page 39).
6. Select **Menu** → **Save** to save the changes.

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

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8 for Smartphone, on another mobile device to create and send an SMS command to your device. As a result, your device receives a covert SMS message 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 Sending a command function:

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

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

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

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

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

CREATING A LIST OF FOLDERS TO DELETE

The Data Wipe function allows creating a list of folders to be deleted after a special SMS command is received.

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

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

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

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

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

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

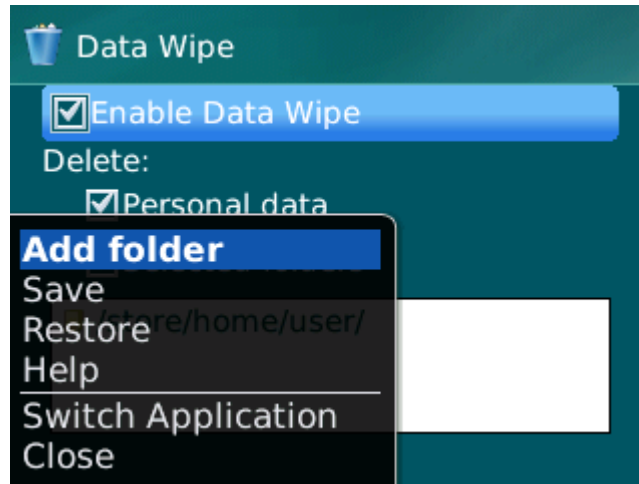


Figure 17: Adding folders

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

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

5. Select **Menu** → **Save**.

➔ *To remove a folder from the list:*

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

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

2. Go to the list of objects for deletion.

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

The confirmation window opens.

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

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

5. Select **Menu** → **Save**.

MONITORING THE REPLACEMENT OF A SIM CARD ON THE DEVICE

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

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

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

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

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

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

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

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

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

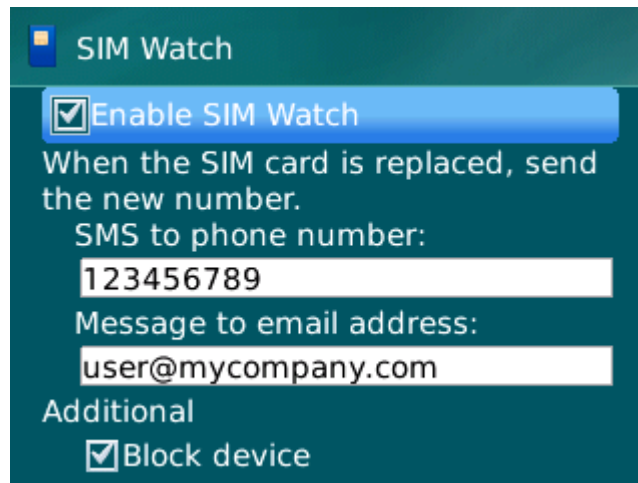


Figure 18: SIM Watch function settings

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

DETERMINING THE DEVICE'S GEOGRAPHICAL COORDINATES

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

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

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

➤ *To enable the GPS Find function:*

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

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

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

After receiving a special SMS command, Kaspersky Endpoint Security 8 for Smartphone sends the device's coordinates by return SMS.

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

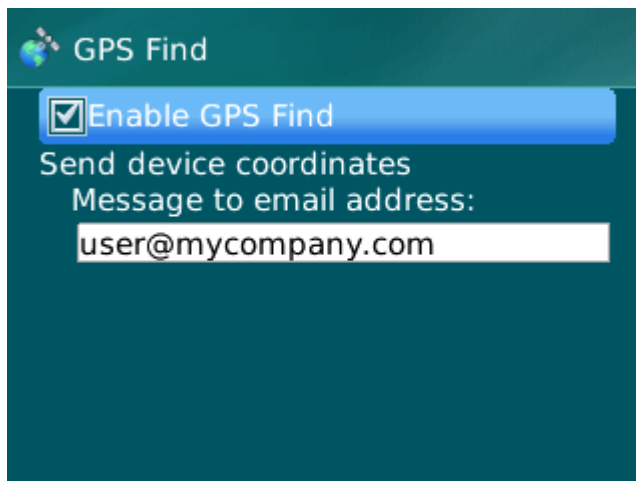


Figure 19: GPS Find function settings

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

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

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8, 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 the SMS, and the application will send the coordinates of the device.

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 Sending a command function:

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

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

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

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

send a standard SMS message 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 has been sent and to an email address if you have previously specified one in the options of GPS Find.

REMOTE START OF THE ANTI-THEFT FUNCTIONS

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

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

- To send an SMS command to another device:

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

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

2. Select the function for remote launch on another mobile device. Select one of the proposed values for the **Select SMS command** setting (see Figure below):
 - **Block device** (on page [36](#)).
 - **Data Wipe** (see "Deleting personal data" section on page [38](#)).
 - **GPS Find** (see the "Determining the device's geographical coordinates" section on page [41](#)).
 - **Privacy Protection** (see section "Hiding personal data" on page [44](#)).

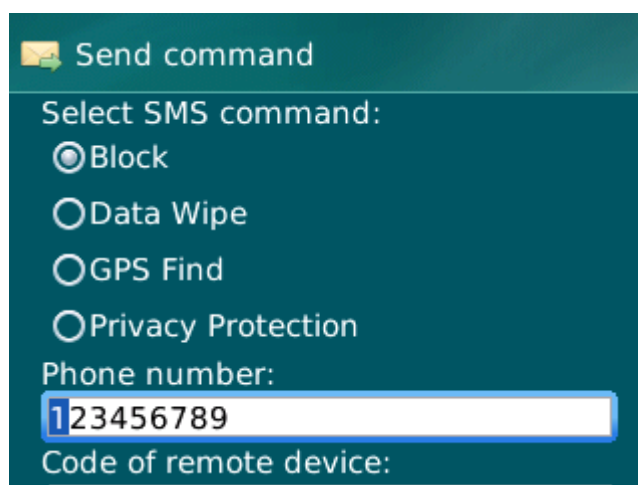


Figure 20: Remote startup of Anti-Theft and Privacy Protection functions

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

PRIVACY PROTECTION

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

IN THIS SECTION

Privacy Protection	44
Privacy Protection modes.....	44
Enabling/disabling Privacy Protection	45
Enabling Privacy Protection automatically.....	45
Enabling Privacy Protection remotely.....	46
Selecting data to hide: Privacy Protection	48
Creating a list of private numbers.....	48

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

Information about the operation of Privacy Protection is stored in the log (see the "Application logs" section on page [50](#)).

PRIVACY PROTECTION MODES

You can manage the operation mode of Privacy Protection. The mode defines whether Privacy Protection is enabled or 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 set Privacy Protection to start automatically (see section "Enabling Privacy Protection automatically" on page [45](#)) or start remotely from another device (see section "Enabling Privacy Protection remotely" on page [46](#)).

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

Changing the mode of Privacy Protection can take some time.

ENABLING/DISABLING PRIVACY PROTECTION

➤ To change the Privacy Protection mode,

select the **Mode** item on the **Privacy Protection** tab (see Figure below).

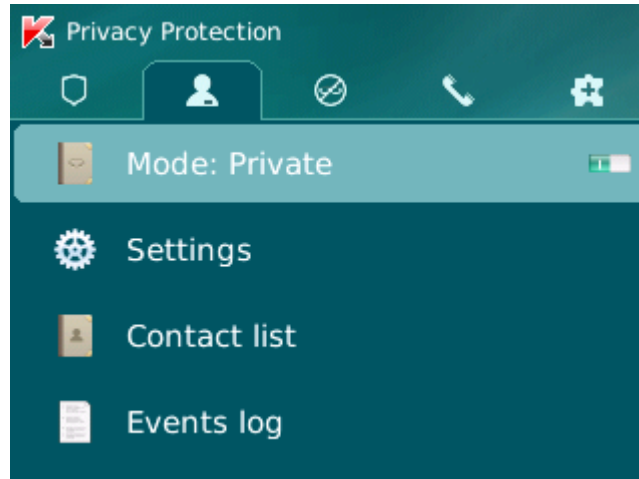


Figure 21: Changing Privacy Protection mode

The current Privacy Protection mode is displayed next to the **Mode** menu item.

The radio button icon to the right of the **Mode** menu item changes according to the selected mode.

ENABLING PRIVACY PROTECTION AUTOMATICALLY

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

Disable Privacy Protection prior to editing Privacy Protection settings.

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

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

This will open the **Settings** window.

2. Check the **Block access** check box in the **Automatic. enabling** (see Figure below).

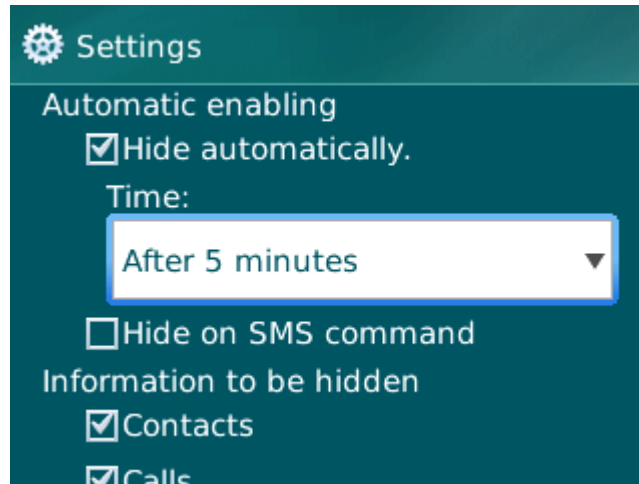


Figure 22: Automatic start of Privacy Protection

3. Select a value for the time interval, which should enable Privacy Protection, when elapsed. To do this, set one of the available values for the **Time** setting:
 - **No delay.**
 - **After 1 minute.**
 - **After 5 minutes.**
 - **After 15 minutes.**
 - **After 1 hour.**
4. Select **Menu** → **Save**.

ENABLING PRIVACY PROTECTION REMOTELY

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

➔ *To allow remote enabling of Privacy Protection:*

1. Select the **Settings** item on the **Privacy Protection** tab.
This will open the **Settings** window.
2. Check the **Hide on SMS command** box (see figure below).

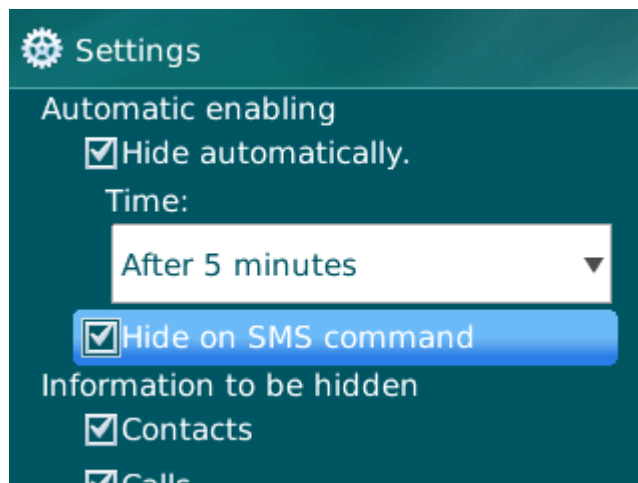


Figure 23: Privacy Protection remote enabling settings

3. Select **Menu** → **Save**.

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

- Use a Kaspersky Lab mobile application, such as Kaspersky Endpoint Security 8 for Smartphone, on another mobile device to create and send an SMS command to your device. As a result, your device unnoticeably receives an SMS, and confidential information is hidden. To create a special SMS command, use the 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, which receives the SMS. As a result, the device receives an SMS, and confidential information is hidden.

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

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

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

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

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

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:

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

SELECTING DATA TO HIDE: PRIVACY PROTECTION

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

Disable Privacy Protection prior to editing Privacy Protection settings.

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

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

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

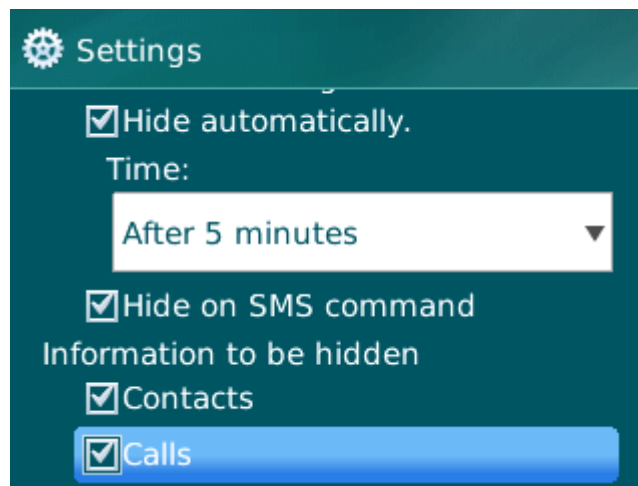


Figure 24: Selecting information and events to hide

2. In the **Information to be hidden** box, select the information and events that are to be hidden for confidential numbers. To do this, check the boxes next to the required settings. The following settings are available:
 - **Contacts** – hide all information about confidential numbers in the Contacts.
 - **Calls** – accept calls from confidential numbers, while not determining the caller's number and not displaying information about confidential numbers in 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.
3. Select **Menu** → **Save**.

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 creating the Contact List, disable hiding confidential information.

IN THIS SECTION

Adding a number to the list of private numbers [49](#)
 Editing a number in the list of private numbers [49](#)
 Deleting a number from the list of private numbers [50](#)

ADDING A NUMBER TO THE LIST OF PRIVATE NUMBERS

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

Before creating the Contact List, disable hiding confidential information.

➔ To add a phone number to the Contact list:

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

The **Contact list** window will open.

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

- To add a number from Contacts, select **Menu** → **Add contact**. When the **Selecting a contact** screen opens, select the required entry from Contacts and select **Menu** → **Select**.
- To add a number manually, select **Menu** → **Add number**. When the **Adding a number** window opens, fill in the **Phone number** and select **Menu** → **Select**.

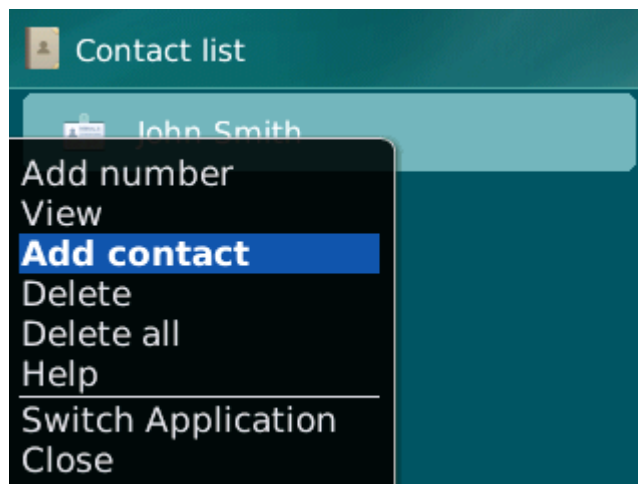


Figure 25: Adding entries to the list of confidential contacts

The number will be added to the Contact list.

EDITING A NUMBER IN THE LIST OF PRIVATE NUMBERS

Disable Privacy Protection prior to editing Privacy Protection settings.

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

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

1. Select the **Contact list** item on the **Privacy Protection** tab.
The **Contact list** window will open.
2. Select a number to edit on the Contact list and then select **Menu** → **Change**.
The **Editing a number** window opens.
3. Change the data in the **Phone number** field.
4. Press **Menu** → **Save** when you have finished editing.

The number is changed.

DELETING A NUMBER FROM THE LIST OF PRIVATE NUMBERS

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

Disable Privacy Protection prior to editing Privacy Protection settings.

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

1. Select the **Contact list** item on the **Privacy Protection** tab.
The **Contact list** window will open.
2. Select a number to be deleted and then select **Menu** → **Delete**.
The confirmation window opens.
3. Confirm deletion. To do this, press **Yes**.

➤ *To clear the Contact List:*

1. Select the **Contact list** item on the **Privacy Protection** tab.
The **Contact list** window will open.
2. Select **Menu** → **Delete all**.
The confirmation window opens.
3. Confirm deletion. To do this, press **Yes**.

The Contact List becomes empty.

APPLICATION LOGS

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

IN THIS SECTION

About logs	51
Viewing Log records.....	51
Deleting Log records	51

ABOUT LOGS

The log stores reports about events occurring when Kaspersky Endpoint Security 8 for Smartphone is running. For every component, a separate events log is used. You are able to select and review a report of activity in the time the component has been running. Entries in the report are sorted in reverse chronological order.

VIEWING LOG RECORDS

➤ *To view the entries in a component's log,*

on the tab of the necessary component, select the item **Events log**.

The selected component's log opens.

Use the scroll bar to scroll through the log.

➤ *To view detailed log record information,*

select the necessary entry and press **ENTER** on the keyboard.

DELETING LOG RECORDS

You can clear all logs. This deletes information about the operation of all Endpoint Security 8 for Smartphone components.

➤ *To clear all logs:*

1. On the tab of any component, select the **Events log**.

The **Events log** window opens.

2. Select **Menu** → **Clear Log**.

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

All entries from all components' logs will be deleted.

CONFIGURING ADDITIONAL SETTINGS

This section gives information about additional features of Kaspersky Endpoint Security 8 for Smartphone: how to change the application secret code, manage the Anti-Spam sound notifications, and enable/disable the display of prompts when configuring the settings for each component.

IN THIS SECTION

Changing the secret code [52](#)
 Displaying prompts..... [52](#)

CHANGING THE SECRET CODE

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

➤ *To change the secret code:*

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

The code entered is automatically verified.

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

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

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

DISPLAYING PROMPTS

When you configure the settings of components, Kaspersky Endpoint Security 8 for Smartphone displays by default a prompt with a short description of the function selected. You can set the display of the program's prompts for Kaspersky Endpoint Security 8 for Smartphone.

➤ *To configure the display of prompts, perform the following steps:*

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

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

GLOSSARY

A

ACTIVATING THE APPLICATION

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

APPLICATION SECRET CODE

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

for access to application settings;

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

B

BLACK LIST

The entries in this list contain the following information:

Phone number from which Anti-Spam blocks calls and / or SMS.

Types of events from this number that Anti-Spam blocks. The following types of events are available: calls and SMS, calls only, and SMS only.

Key phrase that Anti-Spam uses to classify an SMS as unsolicited (spam). Anti-Spam only blocks SMS that contain this key phrase, while delivering all other ones.

D

DELETING SMS MESSAGES

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

N

NON-NUMERIC NUMBER

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

R

REMOTE ADMINISTRATION SYSTEM

The system which remotely manages settings and administers them in real time.

S

SYNCHRONIZATION

Process to connect the mobile device with the remote administration system and transfer data. During synchronization, the application settings configured by the administrator are transferred to the device. Operational reports on the application components are transferred from the device to the remote administration system.

T

TELEPHONE NUMBER MASK

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

W

WHITE LIST

The entries in this list contain the following information:

Phone number from which Anti-Spam delivers calls and / or SMS.

Type of events that Anti-Spam delivers from this number. The following types of events are available: calls and SMS, calls only, and SMS only.

Key phrase used by Anti-Spam to classify an SMS as solicited (not spam). Anti-Spam only delivers SMS that contain this key phrase, while blocking all other ones.

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)

USING THIRD-PARTY CODE

Third party code is used to create the application.

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

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

INDEX

A

Adding	
Anti-Spam Black List	27
Anti-Spam White List	30
list of confidential Privacy Protection numbers	49
Anti-Spam	
action to be performed on a call	35
action to be performed on an SMS message.....	34
Black List	27
modes.....	26
non-numeric numbers.....	33
numbers not in Contacts.....	32
White List.....	29
Anti-Theft	
Block.....	36
Data Wipe.....	38, 39
GPS Find.....	41
SIM Watch.....	40
APPLICATION INTERFACE	23
Application secret code	23, 52
Application tabs.....	24

B

Black List	
Anti-Spam.....	27
Blocking	
device	36
incoming calls	27, 29
incoming SMS messages	27

C

Code	
application secret code	23

D

Data	
remote delete.....	38
DATA	
CONFIDENTIAL INFORMATION	44
Deleting	
Anti-Spam Black List	29
Anti-Spam White List	32
list of confidential Privacy Protection contacts	50
Log records.....	51
Determining the device's location.....	41
Disabling	
Anti-Spam.....	26
Privacy Protection.....	44, 45
Display	
Protection status window	24

E

Editing	
Anti-Spam Black List	28
Anti-Spam White List	31
list of confidential Privacy Protection contacts	49

Enabling	
Anti-Spam.....	26
Privacy Protection.....	45
Entry	
Anti-Spam Black List	27
Anti-Spam White List	30
Events log	
deleting entries	51
viewing entries.....	51
F	
FILTERING	
INCOMING CALLS	25
INCOMING SMS MESSAGES	25
H	
HARDWARE REQUIREMENTS	13
I	
INSTALLING THE APPLICATION	13
K	
KASPERSKY LAB.....	55
L	
License	
information.....	20
installation.....	20
M	
Modes	
Anti-Spam.....	26
Privacy Protection.....	44, 45
P	
Privacy Protection	
automatic start.....	45
list of confidential contacts.....	48
modes.....	44, 45
remote start	46
selecting information and events to be hidden.....	48
Protection status.	24
S	
Send SMS command	43
Starting	
application	22
U	
UNINSTALLING	
APPLICATION.....	18
W	
White List	
Anti-Spam.....	29
Wipe	
information saved on the device	38