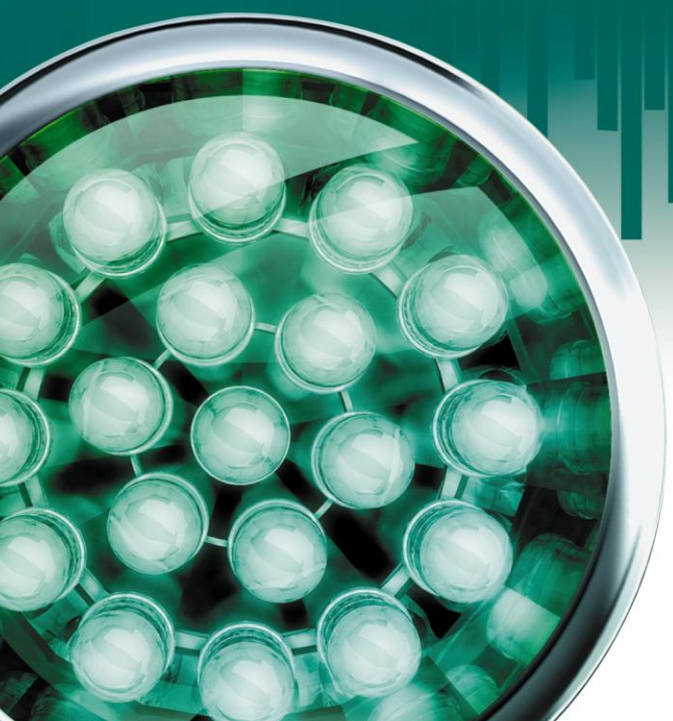
Kaspersky PURE

USER GUIDE

APPLICATION VERSION: 9.0



KASPERSKY lab

Dear User!

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

This document may be amended without additional notification. You can find the latest version of this document at the Kaspersky Lab website, at http://www.kaspersky.com/docs.

Revision date: 12/24/2009

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

LICENSE AGREEMENT

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.

THE SOFTWARE CAN BE ACCOMPANIED WITH ADDITIONAL AGREEMENT OR SIMILAR DOCUMENT ("ADDITIONAL AGREEMENT") WHICH CAN DEFINE NUMBER OF COMPUTERS, WHERE THE SOFTWARE CAN BE USED, PERIOD OF USE OF THE SOFTWARE, TYPES OF OBJECTS WHICH THE SOFTWARE IS INTENDED FOR AND OTHER ADDITIONAL TERMS OF PURCHASE, ACQUISITION AND USE. THIS ADDITIONAL AGREEMENT IS THE INTEGRAL PART OF THE 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.

1.8. **Software Acquisition** means purchase of the Software or acquisition of the Software on terms defined in additional agreement including acquisition at no charge.

2. Grant of License

2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the

Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of computers specified in licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package or as specified in additional agreement.

2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You acquired the License to the Software or as specified in additional agreement.

2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.

2.5. You can transfer the non-exclusive license to use the Software to other individuals within the scope of the license granted from the Rightholder to You provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and substitute you in full in the license granted from the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software including the back-up copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User who acquired the Software from the Rightholder, did.

2.6. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):

- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term

3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.

3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement or as specified in additional agreement.

3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition or as specified in additional agreement.

3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (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 to use the Software without refunding the purchase price or any part thereof.

3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. Technical Support

The Technical Support described in Clause 2.6 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).
Technical support service: http://support.kaspersky.com

5. Information Collection

5.1. Having agreed with the terms and conditions of this Agreement You consent to provide information to the Rightholder about executable files and their checksums to improve Your security protection level.

5.2. In order to improve security awareness about new threats and their sources and in order to improve Your security protection level the Rightholder, with your consent, that has been explicitly confirmed in the Kaspersky Security Network Data Collection Statement, is expressly entitled to receives such information. You can deactivate the Kaspersky Security Network service during installation. Also, You can activate and deactivate the Kaspersky Security Network service at any time in the Software options page.

You further acknowledge and agree that any information gathered by Rightholder can be used to track and publish reports on security risk trends in the Rightholder's sole and exclusive discretion.

5.3. The Software does not process any personally identifiable data and does not combine the processing data with any personal information.

5.4. If you do not wish for the information collected by the Software to be sent to the Rightholder, You should not activate and/or de-activate the Kaspersky Security Network service.

6. Limitations

6.1. 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.

6.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.5 of this Agreement or in additional agreement.

6.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.5 of this Agreement or in additional agreement.

6.4. You shall not rent, lease or lend the Software to any third party.

6.5. 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.

6.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.

6.7. 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.

7. Limited Warranty and Disclaimer

7.1. 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.

7.2. 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.

7.3. 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.

7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.6 of this Agreement.

7.5. 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.

7.6. 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 .

8. Exclusion and Limitation of Liability

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

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

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

9. GNU and Other Third Party Licenses

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

10. Intellectual Property Ownership

10.1 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.

10.2 You acknowledge that the source code, activation code and/or license key file for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.

10.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

11. Governing Law; Arbitration

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration 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.

12. Period for Bringing Actions

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

13. Entire Agreement; Severability; No Waiver

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

14. 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

CONTENTS

ABOUT THIS GUIDE

Kaspersky PURE User Guide contains information about the Kaspersky PURE's principles of operation, the main tasks of home network protection, and the application configuration. This Guide is created for all those who use the Kaspersky PURE application for protecting computers on home networks.

Kaspersky PURE User Guide consists of the following main sections:

- Obtaining information about the application (see page 20). This section describes various sources of information about how to purchase, install and use Kaspersky PURE.
- The concept of Kaspersky PURE (see page 24). This section describes the general concept of comprehensive protection of your home network using various features of the application.
- Installing the application (see page 30). This section provides step-by-step instructions for the correct application installation.
- Getting started (see page 37). This section describes the main operations, which should be performed after the application is installed on your computer, in order to ensure reliable protection.
- Application interface (see page 50). This section describes the application user interface, including the main window, context menu, notification service, and other elements.
- My Computer Protection. This section describes the operation of the components of My Computer Protection designed for protecting your computer from various threats.
- My Backup (see page 181). This section contains the information about backup and data restoration from backup copies.
- My Parental Control (see page 187). This section contains the information about the protection of home network users from threats emerging while working on the computer or surfing the Internet, as well as the information related to the management of Parental Control settings.
- My System Tune-Up. This section contains the information about the wizards and tools that may be useful for advanced protection.
- My Virtual Keyboard (see page 205). This section describes the way of using the virtual keyboard in order to protect your data from key-loggers.
- My Data Encryption (see page 206). This section describes the way of using encrypted containers in order to store confidential data.
- My Password Manager (see page 241). This section describes the way of managing passwords and other personal data.
- My Control Center (see page 241). This section describes the remote management of home network security.
- Configuring Kaspersky PURE (see page 246). This section describes the way of managing the application settings in order to ensure flexible and efficient protection.
- Eliminating problems (see page 265). This section describes the actions that should be taken when any problems occur in the Kaspersky PURE operation.

OBTAINING INFORMATION ABOUT THE APPLICATION

If you have any questions regarding purchasing, installing or using Kaspersky PURE, answers are readily available.

Kaspersky Lab provides various sources of information about the application. You can choose the most suitable of them, with regard to the question importance and urgency.

IN THIS SECTION:

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You may refer to the following sources of information about the application:

- application page at the Kaspersky Lab website;
- application page at the Technical Support Service website (in the Knowledge Base);
- service page of FastTrack Support;
- Help system;
- documentation.

Application page at the Kaspersky Lab website

http://www.kaspersky.com/kaspersky-pure http://www.kaspersky.com/kaspersky-pure

This page will provide you with general information on the application, its features and options.

Application page at the Technical Support Service website (Knowledge Base)

http://support.kaspersky.com/pure http://support.kaspersky.com/pure

On this page, you will find the articles created by Technical Support Service specialists.

These articles contain useful information, recommendations and FAQ on purchasing, installation and use of the application. They are sorted by subject. The articles may provide answers to the questions that concern not only this application but the other Kaspersky Lab products as well; they may also contain the news from Technical Support service.

FastTrack Support service

On this service page, you can find the base of FAQs with answers which is updated on a regular basis. To use this service, you will need an Internet connection.

To go to the service page, in the main application window click the **Support** link, and in the window that will open click the **FastTrack Support** button.

Help system

The application installation package includes the full and context help file that contains the information about how to manage the computer protection (view protection status, scan various computer areas for viruses, execute other tasks), and the information on each application window such as the list of its proper settings and their description, and the list of tasks to execute.

To open the help file, click the **Help** button in the required window, or press the **<F1>** key.

Documentation

Kaspersky PURE installation package includes the **User Guide** document (in PDF format). This document contains descriptions of the application's features and options as well as main operation algorithms.

CONTACTING THE SALES DEPARTMENT

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

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

The service languages are Russian and English.

You can also send your questions to the Sales Department specialists by email sales@kaspersky.com.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

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

In this forum you can view existing topics, leave your comments, create new topics and use the search engine.

KASPERSKY PURE

Kaspersky PURE is a new generation of home network security solutions.

What really sets Kaspersky PURE apart from other software, even from other Kaspersky Lab's products, is the multifaceted approach to the user's home network security.

IN THIS SECTION:

DISTRIBUTION PACKAGE

You can purchase Kaspersky PURE from our partners (boxed edition), or at an online store (e.g., http://www.kaspersky.com, section **eStore**).

If you purchase the boxed product, the distribution package includes the following:

- Sealed envelope with the installation CD where the product files and documentation in PDF format are recorded.
- Printed documentation, namely User Guide and Quick Start Guide.
- License Agreement (depends on the region).
- Activation card that contains the activation code and instructions on application activation (depends on the region).

License agreement is a legal agreement concluded between you and Kaspersky Lab, stating the terms for use of the software product you have purchased.

Please thoroughly read through the License Agreement.

If you do not accept the terms of the License Agreement, you can return your boxed product to the partner from which you have purchased it; in this case, the product will be refunded at the purchase price. However, the envelope with the installation CD (or floppy disks) should remain sealed.

You accept the terms of the License Agreement by unsealing the envelope with the installation CD (or floppy disks).

Before unsealing the envelope with the installation CD (or floppy disks), please thoroughly read through the License Agreement.

When purchasing Kaspersky PURE at eStore, you copy the product from the Kaspersky Lab website. The installation package includes the product itself and this Agreement. The activation code will be sent to you by email when paid.

HARDWARE AND SOFTWARE REQUIREMENTS

For the proper functioning of Kaspersky PURE, your computer should meet the following minimum requirements:

General requirements:

- 320 MB free hard drive space.
- CD-ROM (for installation of Kaspersky PURE from the installation CD).
- Microsoft Internet Explorer 6.0 or higher (for updating application's databases and software modules via Internet).
- Microsoft Windows Installer 2.0.

- *Microsoft Windows XP Home Edition (Service Pack 3),* Microsoft Windows XP Professional (Service Pack 3), Microsoft Windows XP Professional x64 Edition (Service Pack 3)*:*
  - Intel Pentium 300 MHz processor or higher (or a compatible equivalent);
  - 256 MB free RAM.
- *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*
  - Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent);
  - 512 MB free RAM.
- *Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*
  - Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or higher (or a compatible equivalent);
  - 1 GB free RAM (32-bit); 2 GB free RAM (64-bit).

THE CONCEPT OF KASPERSKY PURE

Kaspersky PURE is a program designed for comprehensive protection of computers within your home network. Kaspersky PURE includes the following functional modules:

- My Computer Protection (see page 26), which protects your computer against known and unknown threats;
- My Backup (see page 24), which quickly restores your data if data loss occurs;
- My Encryption (see page 25), which protects your confidential data against unauthorized access;
- My Parental Control (see page 25), which protects children and teenagers from threats related to computer and Internet usage;
- My Password Manager (see page 25), which ensures safe storage of passwords and other account data, and confidentiality while filling various authorization forms;
- My Control Center (see page 25), which allows to remotely manage the security of networked computers;
- My System Tune-Up (see page 26), which is used for optimizing the operating system settings and performing specific computer security tasks.

IN THIS SECTION:

MY BACKUP

Data stored on a computer can be lost due to various issues, such as impact of a virus, information modification or deletion by another user, etc. To avoid losing important information, you should regularly back up data.

Backup copying creates backup copies of objects in a special storage on the selected device. To do so, you should configure backup tasks. After running the task manually or automatically, according to a schedule, backup copies of selected files are created in the storage. If necessary, the required version of the saved file can be restored from the backup copy. Thus, regular backup ensures additional security of data.

SEE ALSO:

MY PARENTAL CONTROL

Parental Control is designed to protect children and teenagers from threats related to computer and Internet usage.

Parental Control allows a flexible limit of the access to resources and applications for different users depending on their age and experience. Besides, this function allows to view statistical reports about the users' actions.

The specified restrictions fall into three categories:

- using the Internet;
- instant messaging;
- using the computer.

SEE ALSO:

My Parental Control.....187

MY CONTROL CENTER

Home network often comprises several computers, which makes it difficult to manage network security. The vulnerability of one computer puts in jeopardy the whole network.

The Control Center allows starting virus scan tasks and update tasks for the whole network or for selected computers, manage the backup copying of data, and configure Parental Control settings on all computers within the network immediately from your workspace. This ensures remote security management of all computers within home network.

SEE ALSO:

My Control Center 241

MY ENCRYPTION

Confidential information, which is saved in electronic mode, requires additional protection from unauthorized access. Storing data in an encrypted container provides this protection.

Data encryption allows creating special encrypted containers on the chosen drive. In the system, such containers are displayed as virtual removable drives. To access the data in the encrypted container, a password should be entered.

SEE ALSO:

My Encryption.....206

MY PASSWORD MANAGER

At the moment, registration and entering account data for authentication are required to access the majority of services and resources. For security reasons, it is not recommended to use identical user accounts for different resources, or write

down your user name and password. As a result, today's user is not able to remember huge amounts of account data, which makes safe storing of passwords particularly up-to-date.

Password Manager makes it possible to store different personal data in encrypted form (for example, user names, passwords, addresses, phone and credit card numbers). Data access is protected with a single Master Password. After entering the Master Password, Password Manager can automatically fill in the fields of different authorization forms. Thus, you should remember only one Master Password to manage all account data.

SEE ALSO:

My Password Manager.....210

MY SYSTEM TUNE-UP

Ensuring computer's security is a difficult task that requires the expertise in operating system's features and in ways of exploiting its weak points. Additionally, volume and diversity of information about system security makes its analysis and processing difficult.

To facilitate solving specific tasks of providing computer security, Kaspersky PURE includes the following wizards and tools:

Browser Configuration Wizard (see page198), which performs the analysis of the Microsoft Internet Explorer settings by assessing them, primarily, in relation to the security.

- System Restore Wizard (see page 199), which removes traces left by malicious objects in the system.
- Privacy Cleaner Wizard (see page 204), which finds and removes traces of user's activities in the system, and the operating system settings, which allow gathering information about the user's activities.
- Rescue Disk (see page 199), which is designed to scan and disinfect infected x86-compatible computers. It should be used when the infection is at such level that it is deemed impossible to disinfect the computer using anti-virus applications or malware removal utilities.
- Permanently Delete Data (see page 202), which prevents unauthorized restoration of deleted files.
- Unused Data Clearing Wizard (see page 203), which deletes temporary and unused files requiring considerable volume of disk space or being at risk of a malware impact.

SEE ALSO:

My System Tune-Up.....198

MY COMPUTER PROTECTION

Computer Protection protects your computer against known and new threats. Each type of threat is processed by a separate application component. This structure of the protection system allows a flexible configuration of the application, depending on the needs of any specific, or of an enterprise as a whole.

Computer Protection includes the following protection tools:

- Protection components (see page 27), which ensure security for:
  - files and personal data;
  - system;

  - network activity.

- Virus scan tasks (on page 29) used to scan individual files, folders, drives, areas, or the entire computer for viruses.

- My Update Center (on page 29), which ensures the up-to-date status of internal application modules and databases used to scan for malicious programs.

PROTECTION COMPONENTS

The following protection components provide defense for your computer in real time:

File Anti-Virus (see page 59)

File Anti-Virus monitors the file system of the computer. It scans all files that can be opened, executed or saved on your computer, and all connected disk drives. Computer Protection intercepts each attempt to access a file and scans such file for known viruses. The file can only be processed further if the file is not infected or is successfully treated by the application. If a file cannot be disinfected for any reason, it will be deleted, with a copy of it saved in the backup, or moved to the quarantine.

Mail Anti-Virus (see page 69)

Mail Anti-Virus scans all incoming and outgoing email messages on your computer. It analyzes emails for malicious programs. The email is available to the addressee only if it does not contain dangerous objects. The component also analyzes email messages to detect phishing.

Web Anti-Virus (see page 76)

Web Anti-Virus intercepts and blocks scripts on websites if they pose a threat. All HTTP traffic is also subject to a thorough monitoring. The component also analyzes web pages to detect phishing.

IM Anti-Virus (see page 83)

IM Anti-Virus ensures the safe use of Internet pagers. The component protects information that comes to your computer via IM protocols. IM Anti-Virus ensures safe operation of various applications for instant messaging.

Application Control (see page 86)

Application Control logs the actions performed by applications in the system, and manages the applications' activities, based on which group the component assigns them to. A set of rules is defined for each group of applications. These rules manage applications' access to various resources.

Firewall (see page 100)

Firewall ensures security for your work in local networks and on the Internet. The component filters all network activities using rules of two types: *rules for applications* and *packet rules*.

Proactive Defense (see page 107)

Proactive Defense allows to detect a new malicious program before it performs its malicious activity. The component is designed around monitoring and analyzing the behavior of all applications installed on your computer. Based on the actions being performed, Computer Protection makes a decision whether the application is potentially dangerous, or not. So your computer is protected not only from known viruses, but from new ones as well that still have not been discovered.

Network Attack Blocker (see page 110)

The Network Attack Blocker loads at the operating system startup, and tracks incoming network traffic for activities characteristic of network attacks. Once an attempt of attacking your computer is detected, Computer Protection blocks any network activity of the attacking computer towards your computer.

Anti-Spam (see page 113)

Anti-Spam integrates into the mail client installed on your computer, and monitors all incoming email messages for spam. All messages containing spam are marked with a special header. The option of configuring Anti-Spam for spam processing (deleting automatically, moving to a special folder, etc.) is also provided. The component also analyzes email messages to detect phishing.

Network Monitor (see page 29)

The component designed to view information about network activity in real-time mode.

Anti-Phishing

The component, integrated into Web Anti-Virus, Anti-Spam and IM Anti-Virus, which allows to check web addresses if they are included in the list of phishing and suspicious web addresses.

Anti-Banner (see page 131)

Anti-Banner blocks advertising information located on banners built into interfaces of various programs installed on your computer, or displayed online.

PROTECTION OF DATA AND ONLINE ACTIVITY

Computer Protection protects data stored on your computer against malware and unauthorized access, ensuring secure access to the local network and to the Internet.

Protected objects are divided into three groups:

- Files, personal data, parameters of access to different resources (user names and passwords), information about banking cards etc. Protection of these objects is provided by File Anti-Virus, Application Control and Proactive Defense.
- Applications installed on your computer and operating system objects. Protection of these objects is provided by Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Application Control, Proactive Defense, Network Attack Blocker and Anti-Spam.
- Online activity: using e-payment systems, email protection against spam and viruses etc. Protection of these objects is provided by Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Firewall, Network Attack Blocker, Anti-Spam, Network Monitor, Anti-Banner.

CONTROL OVER APPLICATIONS AND DATA ACCESS

Computer Protection prevents applications from executing actions which can endanger the system, monitors access to your personal data and provides the option of running applications in the safe mode. It is performed with the help of the following tools:

- **Application Activity Control** (see page 86). The component logs the actions performed by applications in the system, and manages the applications' activities, based on which group they belong to. A set of rules is defined for each group of applications. These rules manage applications' access to various resources.
- **Digital Identity Protection** (see page 89). Application Control manages rights of applications to perform actions on the user's personal data. They include files, folders and registry keys, which contain the settings and important data of the most frequently used applications, as well as user's files (My Documents folder, cookies, information about the user's activity).
- **Safe Run** (see page 95). Computer Protection ensures the maximum security of operating system objects and the user's personal data by running unknown applications in the protected virtual environment.

NETWORK MONITOR

Network Monitor is a tool used to view information about network activities in real time. To run Network Monitor, use the **Network Monitor** link in the Computer Protection main window.

The window that will open will provide the information grouped on the following tabs:

- The *Connections and ports* tab lists all the opened ports and active network connections currently established on your computer.
- The *Firewall: rule processing log* tab displays information about the use of packet rules for applications.
- The *Network traffic* tab displays information on all inbound and outbound connections established between your computer and other computers, including web servers, mail servers, etc.
- The *Blocked computers* tab lists the blocked computers.

VIRUS SCAN TASKS

In addition to the constant protection of all the ways that malicious programs can penetrate, it is extremely important to periodically scan your computer for viruses. This is necessary in order to rule out the possibility of spreading malicious programs that have not been discovered by security components, for example, because the security level was set to low or for other reasons.

The following virus scan tasks are included in Computer Protection:

- **Objects Scan**. Scan of objects selected by the user. You can scan any object in the computer's file system.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Virus scan of operating system startup objects.

UPDATE

To block any network attack, delete a virus or other malicious program, Kaspersky PURE should be regularly updated. The **My Update Center** component is designed for that purpose. It handles the update of application databases and modules used by the application.

The update distribution service allows saving databases and program modules updates downloaded from Kaspersky Lab servers to a local folder and then granting access to them to other computers on the network to reduce network traffic.

INSTALLING KASPERSKY PURE ON YOUR COMPUTER

Kaspersky PURE is installed on the computer in interactive mode using the Installation Wizard that starts when you open the installation file.

Before beginning the installation, you are advised to close all applications currently running.

To install Kaspersky PURE on your computer, run the installation file (file with the .exe extension) on the product CD you have purchased. You can also receive the application installation package via the Internet.

The installation of Kaspersky PURE from the installation package downloaded via the Internet is identical to that from the installation CD.

When the installation package is opened, the application will automatically search for the installation file (with the *.msi extension). If it is found, the application will search for a newer version of the product on Kaspersky Lab servers on the Internet. If the installation package file cannot be found, you will be offered to download it. When the download is complete, the installation of Kaspersky PURE starts. If the download is cancelled, the application installation will proceed in standard mode.

The Installation Wizard is presented as a sequence of windows (steps). To ease the management of the installation process, each window contains the following set of buttons:

- **Next** – accept the action and move to the next step of the installation process.
- **Back** – return to the previous step of the installation process.
- **Cancel** – cancel the installation.
- **Finish** – complete the application installation procedure.

Let us take a closer look at each step of the installation procedure.

IN THIS SECTION:

STEP 1. VERIFYING THAT THE SYSTEM SATISFIES THE INSTALLATION REQUIREMENTS

Before installing Kaspersky PURE, the following items are checked:

- if the operating system and the service packs meet the program requirements for installation;
- if the software required for the proper functioning of Kaspersky PURE is installed on the computer;
- if the user has rights to install the software.

If the check is successfully completed, the Kaspersky PURE Installation Wizard window opens.

If a condition is not met, a notification with the problem description will appear on the screen. In this case, before installing the Kaspersky Lab's application, you are advised to install all necessary applications and the required service packs using the Windows Update service.

STEP 2. SELECTING THE TYPE OF THE INSTALLATION

If the computer meets the system requirements, the Installation Wizard window will open. You will be offered to select one of the following installation modes:

- *Express installation*. When this option is selected (the **Custom installation** box is unchecked), the application will be installed on your computer in its entirety. The protection settings recommended by Kaspersky Lab will be applied. When the installation is completed, you can activate Kaspersky PURE and then configure the application protection against unauthorized access.
- *Custom installation*. In this case (the **Custom installation** box is checked), you can modify the default installation settings. You can select which application components should be installed and specify the folder where the application will be installed. The protection settings recommended by Kaspersky Lab will be specified for each component you have selected. When the installation is completed, you can activate the application and configure the protection against unauthorized access.

> The custom installation mode is recommended for experienced users only.

If you select the first option, the Application Installation Wizard will offer you to view the License Agreement and the Kaspersky Security Network Data Collection Statement. After that, the application will be installed on your computer.

If you select the second option, you will be asked to enter or to confirm certain information at each step of the installation.

To proceed with the installation, click the **Next** button. To cancel the installation, click the **Cancel** button.

STEP 3. ACCEPTING THE LICENSE AGREEMENT

Before installing the application, you will be offered to view the License Agreement concluded by you and Kaspersky Lab. The License Agreement lists the user's rights to use the software he or she has purchased. Without accepting the terms of the License Agreement, you cannot proceed with the application installation.

Please read the agreement carefully, and if you accept each of its terms, click the **I agree** button. The application installation will go on.

To cancel the application installation, click the **Cancel** button.

STEP 4. PARTICIPATING IN THE KASPERSKY SECURITY NETWORK PROGRAM

You can participate in the Kaspersky Security Network program. The purpose of the program consists in revealing new threats to data security and improve the quality of Kaspersky Lab's products. To help us do it, you can provide our company the right of using the information about the status of your computer's security and the threats you have detected. To perform the analysis, you can also send information about the operating system and the unique identifier, which is assigned to your computer by Kaspersky PURE.

Kaspersky Lab guarantees that no personal data will be used.

Please view the regulations concerning the participation in Kaspersky Security Network. If you accept all terms of it, check the **I accept the terms of participation in Kaspersky Security Network** box.

Click the **Next** button. The installation will continue.

STEP 5. SELECTING THE DESTINATION FOLDER

This step is available if the custom selection of Kaspersky PURE is selected (see page 31).

At this step, you can select the destination folder into which Kaspersky PURE should be installed. The default path for the application installation is as follows:

- **<drive> \ Program Files \ Kaspersky Lab \ Kaspersky PURE** – for 32-bit systems;
- **<drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky PURE** – for 64-bit systems.

To change the destination folder, click the **Browse** button and specify a different folder in the window that will open. You can also specify a new installation path, by entering it in the **Destination folder** field.

Please remember that if you enter the full path to the installation folder manually, it should not contain more than 200 characters or include any special characters.

Click the **Next** button. The installation will continue.

STEP 6. SELECTING APPLICATION COMPONENTS FOR THE INSTALLATION

This step is available if the custom selection of Kaspersky PURE is selected (see page 31).

At this step, you can select the application components that will be installed on your computer. By default, all the protection components and the program kernel are selected.

To make a decision on installing a component, you can view a brief description of the component you have selected shown in the bottom part of the window, and find out how much free disk space is required to install this component.

To select a component for installation, open the menu by left-clicking the icon next to the name of the component and select the **This feature will be installed on the local hard drive** item.

To obtain detailed information about free disk space on your computer, click the **Volume** button. Information will be displayed in the window that will open.

To cancel the installation of a component, select the **This feature will become unavailable** option from the context menu. Note that if you cancel installation of any component you will not be protected against a number of hazardous programs.

When you have finished selecting components to be installed, click the **Next** button. To return to the default list of components to be installed, click the **Reset** button.

STEP 7. SEARCHING FOR OTHER ANTI-VIRUS APPLICATIONS

At this step, the wizard searches for other anti-virus programs, including other Kaspersky Lab's programs, which may conflict with Kaspersky PURE.

If any anti-virus applications were detected on your computer, they will be listed on the screen. You will be asked to uninstall them before you proceed with the installation.

To remove the anti-virus programs that you have detected, use the **Remove** button.

To proceed with the installation, click the **Next** button.

STEP 8. DISABLING MICROSOFT WINDOWS FIREWALL

This step is only performed if the My Computer Protection module is being installed on a computer with Microsoft Windows Firewall enabled, and Firewall is among the application components which you wish to install.

At this step of the installation of Kaspersky PURE, you are offered to disable the firewall integrated into Microsoft Windows. The My Computer Protection module includes the Firewall component, which ensures comprehensive protection of your network activities. So, there is no need to use additional protection provided by the operating system.

If you want to use Firewall as the main protection tool for network activity, click the **Next** button. Microsoft Windows firewall will be disabled automatically.

If you want to protect your computer with Microsoft Windows firewall, select the **Keep Microsoft Windows Firewall enabled** option. In this case, the Firewall component will be installed but disabled to avoid conflicts in the application's operation.

STEP 9. FINAL PREPARATION FOR INSTALLATION

This step completes the preparation for installing Kaspersky My Computer Protection on your computer.

At the initial and custom installation (see page 31) of the application, please do not uncheck the **Protect the installation process** box. If any errors occur during the application installation, enabling the protection will allow you to perform a correct procedure of installation rollback. When you retry the installation, we recommend that you uncheck this box.

If the application is being remotely installed using *Windows Remote Desktop*, you are advised to uncheck the **Protect the installation process** box. If this box is checked, the installation procedure may be left unfinished or performed incorrectly.

To proceed with the installation, click the **Install** button.

When installing Kaspersky PURE components which intercept network traffic, current network connections will be terminated. The majority of terminated connections will be restored after a pause.

Kaspersky PURE Configuration Wizard will automatically start after the installation.

MODIFYING, RESTORING, AND REMOVING THE APPLICATION WITH THE INSTALLATION WIZARD

Restoring the application may be useful if you have detected some errors in its operation, which have occurred due to an incorrect configuration or corrupted files.

Changing the set of components allows you to install new Kaspersky PURE components or remove those hampering your work or those you find unnecessary.

- *To begin restoring the original state of the application, installing Kaspersky PURE components that have not been installed before, or removing the application:*

  1. Insert the installation CDinto the CD/DVD-ROM if you have already used it to install the application. If you install Kaspersky PURE from a different source (shared folder, folder on the hard drive, etc.), please make sure that the installation package is available from that source and you have access to it.

  2. Select **Start** → **Programs** → **My Computer Protection** → **Modify, Repair or Remove installation**.

This launches the installation program, which functions as a wizard. Let us view the detailed procedure for restoring the application, modifying the set of components, or removing the application.

IN THIS SECTION:

STEP 1. STARTING WINDOW OF THE INSTALLATION PROGRAM

If you have performed all the afore-mentioned actions required for restoring the application or modifying the set of its components, the welcoming window of the Kaspersky PURE installation program will open. To proceed, click the **Next** button.

STEP 2. SELECTING OPERATION

At this step, you should select which action on the application you want to take: you will be offered to modify the set of application components, restore the original state of the components you have installed before, or remove some components or the entire application. To take the required action, click the corresponding button. Further steps of the installation program depend on the operation you have selected.

Modification of the set of components is performed similarly to the custom installation of the application: you can specify which components are to be installed and select the ones you want to exclude.

Restoration of the application is performed based on the set of components installed. The application will update the files of all components that have been installed; the **Recommended** protection level will be set for each of them.

When removing the application, you can select which data items created and used by the application you want to save on your computer. To delete all data of Kaspersky PURE, select the **Complete uninstall** option. To save the data, select the **Save application objects** option and specify which objects should remain intact:

- *Keep activation data* – key file required for the functioning of the application.
- *Anti-Spam databases* – database used for recognizing unsolicited email messages. This database contains detailed information used to tell spam messages from useful ones.
- *Keep backup and quarantine files*. Backup objects are backup copies of the objects you have deleted or disinfected. We recommend that you save such objects so that they can be restored in the future. Quarantine objects are those probably infected with viruses or their modifications. Such objects contain code which is similar to that from a known virus; however, we cannot affirm their maliciousness unambiguously. We recommend that you save them since they may turn out to be uninfected, or become disinfectible after the application databases are updated.
- *Keep protection settings* – values set for the parameters of all the application components.
- *Keep iSwift and iChecker data* – database that contains information about scanned NTFS objects. It allows accelerating the object scan. By using the data from this database, Kaspersky PURE only scans the objects that have been modified since the last scan.
- *Keep data of Safe Run Shared Folder* – data which are accessible both in Safe Run and in common run mode.

If a considerable time interval has elapsed between the moment you had removed an older version of Computer Protection and the moment you had installed a newer one, we recommend that you abstain from using the iSwift и iChecker database saved since the previous installation of the application. During this time interval, a malicious program may have penetrated into your computer and taken malicious actions that cannot be detected with this database, which may eventually lead to the infection of your computer.

To start the operation you have selected, click the **Next** button. This launches the process of copying the required files to your computer or removing the components and data you have selected.

STEP 3. FINISHING APPLICATION MODIFICATION, RESTORATION, OR REMOVAL

The process of restoration, modification or removal is displayed on the screen, and you are notified of its completion.

As a rule, the removal requires that you restart your computer since it is necessary for applying the changes to the system. The request for restarting the computer will be displayed on the screen. Click the **Yes** button to restart your computer immediately. To restart your computer manually later, click the **No** button.

GETTING STARTED

One of the main goals of Kaspersky Lab when creating Kaspersky PURE was comprehensive protection of computers within home network. The optimal configuration of all application settings allows users with any level of computer literacy to ensure his or her computer's protection immediately after the installation.

For the users' convenience, the initial configuration stages are combined in the interface of the Application Configuration Wizard (see section "Application Configuration Wizard" on page 38), which starts after the installation is complete. Following the wizard's instructions, you will be able to activate Kaspersky PURE, modify the update settings, restrict access to the application using a password, and edit other settings.

Your computer may turn out to be infected with malware before the installation of Kaspersky PURE. To detect the malware on your computer, run the full computer scan (see section "Scanning computer for viruses" on page 43).

As a result of malware operation and system failures, the settings of your computer can be corrupted. Run the vulnerability scan task (see section "Scanning computer for vulnerabilities" on page 43) to find the vulnerabilities of the installed software and anomalies in the system settings.

At the moment of application installation, databases included in the installation package may become outdated. Start the application update (on page 42) (unless it has been done using the setup wizard or automatically immediately after the application had been installed).

The Anti-Spam component included in the Computer Protection package uses a self-training algorithm to detect unwanted messages. Run the Anti-Spam Training Wizard (see section "Training using the Training Wizard" on page 116) to configure the component for working with your email.

If data loss occurs, for quick data restoration, configure the backup tasks (see section "My Backup" on page 48).

To protect confidential information against unauthorized access, create encrypted containers for data storage (see section "My Encryption" on page 48).

To protect children and teenagers from threats related to computer usage, specify Parental Control restrictions (see section "My Parental Control" on page 48).

After completion of the above actions, Kaspersky PURE will be ready for the operation. To evaluate the level of your computer protection, use Security Management Wizard.

IN THIS SECTION:

APPLICATION CONFIGURATION WIZARD

The Application Configuration Wizard starts after the installation is complete. It is designed to help you configure the initial settings of Kaspersky PURE, based on the features and tasks of your computer.

The Application Configuration Wizard's interface is a series of steps in windows that you can navigate, using the **Back** button and the **Next** link, or close using the **Cancel** button.

LET US TAKE A CLOSER LOOK AT THE WIZARD'S STEPS

STEP 1. ACTIVATING THE APPLICATION

The application activation procedure consists in registering a license by installing a key file. Based on the license, the application will determine the existing privileges and calculate its term of use.

The key file contains service information required for Kaspersky PURE to be fully functional, and additional data:

- support information (who provides the support, and where it can be obtained);
- key file name and number, and the license expiration date.

You will need an Internet connection to activate the application.

To obtain a key file at the activation, you should have an activation code. Activation code is provided when you purchase the application. You will be offered the following options of Kaspersky PURE activation:

- **Activate commercial license**. Select this activation option if you have purchased a commercial version of the application, and you have been provided an activation code. You can use this code to obtain a key file providing access to the application's full functionality throughout the effective term of the license.
- **Activate trial license**. Use this activation option if you want to install the trial version of the application before making the decision to purchase a commercial version. You will be provided a free key file valid for a term specified in the trial version license agreement.
- **Activate later**. If you select this option, the stage of Kaspersky PURE activation will be skipped. The application will be installed on your computer, but you will not be able to use certain application functions, for example update (you will be able to update the application only once after its installation), creation of an encrypted container, additional tools, etc. The **Activate later** option is only available at the first start of Activation Wizard, immediately after the application installation.

If Kaspersky PURE has been installed and then removed with activation information saved, this step will be skipped. In this case, Configuration Wizard will automatically receive information about the existing license which will be displayed in the wizard window.

SEE ALSO:

ACTIVATING THE COMMERCIAL VERSION

If you select this option, the application will be activated from a Kaspersky Lab's server that requires an Internet connection.

Activation is performed by entering an activation code that you receive by email when you purchase Kaspersky PURE via Internet. If you purchase the application in a box (retail version), the activation code will be printed on the inner face of the disk envelope cover or under the protective layer of the sticker on the inner face of the DVD box.

The activation code is a sequence of digits divided by hyphens into four groups of five symbols without spaces. For example, 11111-11111-11111-11111. Note that the code should only be entered in Latin characters.

Activation Wizard establishes connection with a Kaspersky Lab's activation server on the Internet, and sends it your activation code, after which the code is verified. If the activation code has passed the verification successfully, the Wizard receives a key file which then will be installed automatically. The activation process completes accompanied by a window with detailed information about the purchased license.

If the activation code has not passed the verification, you will see the corresponding message on the screen. In this case, you should contact the software vendor from which you have purchased Kaspersky PURE.

If the number of activations with the activation code has been exceeded, the corresponding notice will pop up on the screen. Activation process will be interrupted, and the application will offer you to contact Kaspersky Lab's Technical Support service.

If any errors have occurred when connecting to an activation server, and if you cannot obtain a key file, please contact the Technical Support Service.

ACTIVATING THE TRIAL VERSION

Use this activation option if you want to install a trial version of Kaspersky PURE before making the decision to purchase a commercial version. You will be provided a free key file valid for a term specified in the trial version license agreement. When the trial license is expired, it cannot be activated for the second time.

If any errors have occurred when connecting to an activation server, and if you cannot obtain a key file, please contact the Technical Support Service.

COMPLETING THE ACTIVATION

The Activation Wizard will inform you that Kaspersky PURE is successfully activated. Additionally, information about the license is provided: license type (commercial, trial), expiration date, and number of hosts for the license.

STEP 2. RESTRICTING ACCESS TO THE APPLICATION

The purpose of access restriction consists in preventing unauthorized attempts of disabling the protection or modifying the settings of the components integrated into Kaspersky PURE.

Restricting access to Kaspersky PURE with a password may be useful in the following cases:

- if a personal computer is used by several persons, probably with varying levels of computer literacy;
- if Kaspersky PURE ensures security of several computers joined into a home network;
- if protection is at the risk of being disabled by malware.

To enable password protection, check the **Enable password protection** box and fill in the **Password** and **Confirm password** fields.

Below, specify the area that you want to protect with a password:

- **Application settings configuration** – the password will be requested when the user attempts to save changes made to Kaspersky PURE settings.
- **My Backup management** – the password will be requested before the backup tasks are run.
- **My Parental Control management** – the password will be requested before the backup tasks are run.
- **My Control Center management** – the password will be requested before modifying the Kaspersky Pure settings via the network.
- **Exiting the application** – the password will be requested when the user attempts to exit the application.

STEP 3. SELECTING PROTECTION MODE

This step of the Application Configuration Wizard will be skipped if you have selected the quick install mode. The application settings edited at this step will be assigned the default values.

Select the protection mode provided by Kaspersky PURE.

Two modes are available:

- *Automatic*. If any important events occur, Kaspersky PURE automatically performs the action recommended by Kaspersky Lab. Once a threat is detected, the application attempts to disinfect the object; if it fails, the application deletes it. Suspicious objects will be skipped without processing. Pop-up messages inform the user about new events.

- *Interactive*. In this mode the application reacts to events in the manner you have specified. Once an event requiring your attention occurs, the application displays notifications which offer you to select an action.

Notifications warning about the detection of an active infection are displayed irrespective of the protection mode you have selected.

STEP 4. CONFIGURING APPLICATION UPDATE

This step of the Application Configuration Wizard will be skipped if you have selected the quick install mode. The application settings edited at this step will be assigned the default values.

The quality of your computer's protection depends directly on regular updates of the databases and application modules. In this window, the Configuration Wizard asks you to select the update mode and to specify the schedule settings.

- **Automatic update**. The application checks the update source for update packages at specified intervals. Scanning frequency can be increased during anti-virus outbreaks and decreased when there are none. Having discovered new updates, the program downloads and installs them on the computer. This is the default mode.

- **Scheduled updates** (time interval may change depending on the schedule settings). Updates will run automatically according to the schedule created. You can alter the schedule settings in the window that will open by clicking the **Settings** button.

- **Manual updates**. If you select this option, you will run application updates on your own.

Note that the databases and application modules included with the installation package may be outdated by the time you install Kaspersky PURE. You are advised to obtain the latest updates. To do so, click the **Update now** button. In this case the application will download the necessary updates from update servers, and install them on your computer.

If the databases included with the installation package are obsolete, the update package may be large-sized so that it may cause the additional Internet traffic (up to several tens of Mb).

If you want to switch to editing the update settings (select the resource from which the updates will be downloaded, or the user account used to run the update process, etc.), click the **Settings** button.

STEP 5. SELECTING THREATS TO BE DETECTED

This step of the Application Configuration Wizard will be skipped if you have selected the quick install mode. The application settings edited at this step will be assigned the default values.

At this step, you can select the threat categories to be detected by the Computer Protection module. Computer Protection always detects programs that are capable of damaging your computer. including viruses, worms and Trojans.

STEP 6. ANALYZING THE APPLICATIONS INSTALLED ON THE COMPUTER

At this stage, information about Microsoft Windows applications is collected. These applications are added to the list of trusted applications which have no restrictions imposed on the actions they perform on the system.

Other applications are analyzed after they are started for the first time when Kaspersky PURE has been installed.

STEP 7. CLOSING CONFIGURATION WIZARD

The last window of the Wizard will inform you of a successful completion of application installation. To run Kaspersky PURE, make sure that the ☑ **Run Kaspersky PURE** is checked, and click the **Finish** button.

SELECTING NETWORK TYPE

After Kaspersky PURE is installed, the Firewall component will analyze your computer's active network connections. Each network connection will be assigned a status which determines the allowed network activities.

If you have selected the interactive mode of Kaspersky PURE operation (see section "Step 3. Selecting protection mode" on page 41), a notification will appear each time a new network connection is detected. You can select the status for the new network in the notification window:

- **Public network**. Network connections with this status are denied access to your computer from the outside. In such networks access to public folders and printers is denied. This status is recommended for connections to the Internet network.
- **Local network**. Network connections with this status are allowed access to public folders and network printers. You are advised to assign this status to protected local networks, for example, a corporate network.
- **Trusted network**. Network connections with this status are not restricted. You are advised to assign this status only to absolutely secure areas.

For each network status, Kaspersky PURE uses an associated set of rules to manage the network activity. Later if necessary you can change a connection's network status from that initially specified.

UPDATING THE APPLICATION

You will need an Internet connection to update Kaspersky PURE.

Kaspersky PURE relies upon the application databases which contain threat signatures, characteristic spam phrases, and descriptions of network attacks. At the moment Kaspersky PURE is installed these databases may be obsolete, since Kaspersky Lab updates both the databases and application modules on a regular basis.

When Application Configuration Wizard is active, you can select the update launch mode (see section "Step 4. Configuring application update" on page 41). By default, Kaspersky PURE automatically checks for updates on Kaspersky Lab's update servers. If the server contains a fresh set of updates, Kaspersky PURE will download and install them in the silent mode.

If the databases, included in the installation package, are outdated, the update package can be large and it can cause the additional internet traffic (up to several tens of Mb).

To keep your computer's protection up to date, you are advised to update Kaspersky PURE immediately after the installation.

To manually update Kaspersky PURE, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the left part of the window that will open, select the **My Update Center** section.
3. Click the **Start update** button.

SCANNING COMPUTER FOR VIRUSES

Developers of malware make every effort to conceal the actions of their programs, and therefore you may not notice the presence of malware on your computer.

After Kaspersky PURE has been installed, it automatically performs a **Quick scan** of your computer. This task searches for and neutralizes harmful programs in objects loaded during operating system startup.

Kaspersky Lab's specialists also recommend that you perform the **Full Scan** task.

To start a virus scan task, perform the following actions:

1. Open the main application window and click the **My Computer Protection**.
2. In the left part of the window that will open, select the **Scan My Computer** section.
3. Click the **Start Full Scan** button to start the scan.

SCANNING COMPUTER FOR VULNERABILITIES

The settings of your operating system can become corrupted by system failures, or by the activities of malicious programs. Additionally, user applications installed on your computer can have vulnerabilities which intruders can use to damage your computer.

In order to detect and eliminate such problems, you are advised to launch the *Vulnerability Scan task* (see page 144) after you have installed the application. During task execution the search is performed for vulnerabilities in installed applications, as well as for damages and anomalies in the operating system and browser settings.

To start the vulnerability scan task:

1. Open the main application window and click the **My Computer Protection**.
2. In the left part of the window that will open, select the **Scan My Computer** section.
3. Click the **Open Vulnerability Scan window** button.
4. In the window that will open, click the **Start Vulnerability Scan** button.

MANAGING LICENSE

Kaspersky PURE needs a valid key to operate. A key file is provided using the activation code obtained when purchasing the application, it ensures the right to use it since the date of activation. The key file contains information about the license: the type, the expiration date, and the number of hosts.

Without a key file, unless a trial version of the application has been activated, Kaspersky PURE will run with limited functionality. For example, only one application update will be available after the installation (the application will not

download any new updates). A number of other application functions will also be not available, for example, additional tools, creation of an encrypted container, etc.

If a trial version of the program has been activated, after the trial period expires, Kaspersky PURE will not run.

When the commercial license expires, the application also switches to the mode of limited functionality, in which My System Tune-Up and a number of other functions are not available. As before, you will be able to scan your computer for viruses and use the protection components, but only using the databases that you had when the license expired. We cannot guarantee that you will be protected from viruses that surface after your application license expires.

To protect your computer from infection with new viruses, we recommend that you renew your license for Kaspersky PURE. Two weeks prior to the license expiration the application will notify you about it. During some time a corresponding message will be displayed each time the application is launched.

Information about the license currently in use is displayed in the **License manager** window: its type (commercial, commercial with subscription, commercial with protection subscription, trial), the maximum number of hosts, the expiration date, and the number of days remaining. Information about the license expiration term will not be displayed if the commercial license with subscription or the commercial license with protection subscription is installed.

To view the provision of the application license agreement, click the **View End User License Agreement** button. To delete the key file, click the  button to the right of the license whose key file you wish to delete. To activate a new license, click the **Activate new license** button.

Using the **Purchase license** (**Renew license**) button, you can proceed with purchasing (renewing) the license in Kaspersky Lab's e-Store.

Kaspersky Lab has regular special pricing offers on license extensions for our products. Check for special offers on the Kaspersky Lab website, in the **Products & Services** → **Sales and special offers** section.

PARTICIPATING IN KASPERSKY SECURITY NETWORK

A great number of new threats appear worldwide on a daily basis. To facilitate the gathering of statistics about new threats, their source and to help in developing methods to be used for their elimination, Kaspersky Lab invites you to use the Kaspersky Security Network service.

The use of the Kaspersky Security Network involves sending the following information to Kaspersky Lab:

- A unique identifier assigned to your computer by Kaspersky PURE. which characterizes the hardware settings of your computer and does not contain any information.
- Information about threats detected by application's components. The information's structure and contents depend on the type of the threat detected.
- Information about the system: operating system's version, installed service packs, services and drivers being downloaded, versions of browsers and mail clients, browser extensions, version number of the Kaspersky Lab's application installed.

Kaspersky Security Network also gathers extended statistics, including information about:

- executable files and signed applications downloaded on your computer;
- applications run on your computer.

The statistical information is sent once application updating is complete.

Kaspersky Lab guarantees that no gathering and distribution of users' personal data is performed within Kaspersky Security Network.

To configure the statistics sending settings:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. Select the **Feedback** section in the left part of the window.
3. Check the **I agree to participate in Kaspersky Security Network** box to confirm your participation in Kaspersky Security Network.

SECURITY MANAGEMENT

Problems in computer protection are indicated by the computer protection status (see section "My Computer Protection" on page 53), which is displayed by changes in the color of the protection status icon, and of the panel in which this icon is located. Once problems appear in the protection system, you are advised to fix them immediately.

Figure 1. Current status of the computer protection

You can view the list of problems occurred, their description, and possible methods of resolving, on the **Status** tab (see figure below); you can select it by clicking on the status icon or on the panel on which it is located (see figure above).

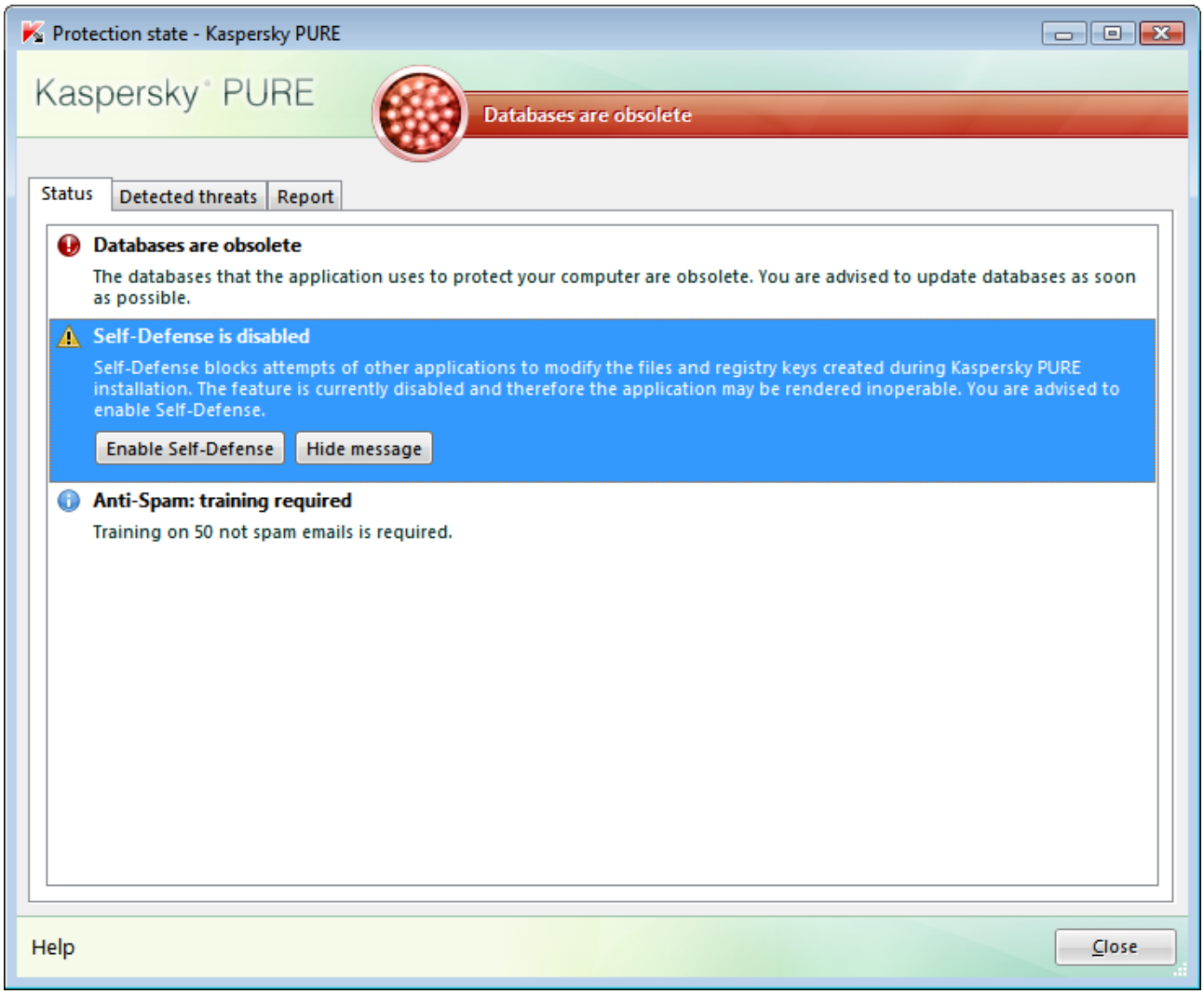


Figure 2. Solving security problems

The tab shows the list of current problems. The problems are sorted with regard to their criticality: first, the most critical ones (i.e., with red status icon), then less critical ones – with yellow status icon, and the last – information messages. A detailed description is provided for each problem and the following actions are available:

- *Eliminate immediately*. Using the corresponding buttons, you can switch to fix the problem, which is the recommended action.

- *Postpone elimination*. If, for any reason, immediate elimination of the problem is not possible, you can put off this action and return to it later. To do so, click the **Hide message** button.

  Note that this option is not available for serious problems. Such problems include, for example, malicious objects that were not disinfected, crashes of one or several components, or corruption of the program files.

To make hidden messages re-appear in the general list, check the **Show hidden messages** box.

PROTECTION STATUS

Performance of Kaspersky PURE components or of virus scan tasks is logged in the report which contains summary information about the computer protection status. There you can learn how many dangerous and suspicious objects have been detected by the application, and find out which of them have been disinfected, deleted, or quarantined.

The Computer Protection status (see section "My Computer Protection" on page 53) warns the user about the malicious objects detected by the application, by changing the color of the protection status icon and that of the panel on which it is located. If malicious objects are detected, the color of the icon and the panel will change to red. In this case, all emerging threats should be eliminated immediately.

To view information on the computer protection status:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that opens, click the **Report** link.

To eliminate problems occurred in the computer protection:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that opens, click the **Report** link.
3. In the window that opens, on the **Status** tab, perform the required actions. To make hidden messages re-appear in the general list, check the **Show hidden messages** box.

In order to perform an action on a detected object:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that opens, click the **Report** link.
3. In the window that opens, on the **Detected threats** tab, select the required object in the list of objects and right-click it to open its context menu.
4. Select the required action in the context menu that will open.

To view the report on protection components operation:

1. Openthe main application window and click the **My Computer Protection** button.
2. In the window that opens, click the **Report** link.
3. In the window that opens, select the **Report** tab.

PAUSING PROTECTION

Pausing protection means temporarily disabling all protection components for a certain period of time.

As a result of temporarily disabling protection, all protection components will be paused. This is indicated by:

- inactive (grey) application icon (see section "Notification area icon" on page 50) in the taskbar notification area;
- red color of the status icon and the panel of the main Kaspersky PURE window.

If network connections were established at the same time as the protection was paused, a notification about termination of such connections will be displayed.

To pause the protection of your computer:

1. In the context menu (see section "Context menu" on page 50) of the application, select **Pause protection**.

2. In the **Pause protection** window that opens, select the time interval after which the protection should be resumed:

   - **Pause for the next <time interval> –** protection will be enabled in a specified amount of time. Use the dropdown menu to select the time interval value.

   - **Pause until reboot –** protection will be enabled after application restart or after the system restart (provided that Kaspersky PURE is set to start automatically on startup).

   - **Pause** – protection will be enabled only after you start it manually. To enable protection, select the **Resume protection** item from the application's context menu.

MY BACKUP

The most common way to protect important data from being lost is to regularly back it up. You are recommended to configure backup tasks to regularly save up-to-date information.

Before you can start working, you should create a backup storage (see section "Creating a backup storage area" on page 181) on the selected drive. The backup copies of required files will be created in this storage. After that, you can configure backup tasks (see section "Creating a backup task" on page 183) (select files for which backup tasks should be created, configure the automatic startup schedule and other backup conditions).

MY PARENTAL CONTROL

Immediately after Kaspersky PURE installation, Parental Control is disabled. No restrictions are set for the users. To protect children and teenagers from threats related to computer and Internet usage, you should timely configure Parental Control settings for all users.

If you have not enabled password protection when installing the application (see section "Step 2. Restricting access to the application" on page 40), at the first startup of Parental Control you are recommended to set a password for protection from unauthorized modification of the Control settings. After that, you can enable Parental Control and impose restrictions (see section "Enabling and configuring Parental Control" on page 188) on computer and Internet usage, and on instant messaging for all accounts on the computer.

MY ENCRYPTION

To protect confidential information from unauthorized access, you are recommended to store it in encrypted form in a special container.

Before you can start working, you should create an encrypted container (see section "Creating container" on page 206), write data into it (see section "Adding files into container" on page 208) as on a standard removable drive, and then disconnect (see section "Connecting and disconnecting container" on page 207) the container. After that, a password should be entered to connect the container and access the data.

MY PASSWORD MANAGER

Password Manager protects your personal data and makes it easy to manage.

One of the features of the application is the optimal configuration of its initial parameters. For users' convenience, the initial configuration stages are combined in the interface of the Application Configuration Wizard (see page 213), which

opens at the first startup of the application. Following the wizard's instructions, you can create a Master Password, modify the settings for accessing the application and protecting your data.

To prevent unauthorized access to your personal data when you are away from your computer, Password Manager automatically locks the Password Database. To use your personal data, unlock Password Manager (see page 214).

Password Manager helps you use (see page 221) and manage your personal data. To find any information you have saved, start the password search (see page 222).

APPLICATION INTERFACE

Kaspersky PURE has a fairly simple and easy-to-use interface. This section will discuss its basic features in detail.

IN THIS SECTION:

NOTIFICATION AREA ICON

Immediately after installing Kaspersky PURE, its icon will appear in the Microsoft Windows taskbar notification area.

This icon is an indicator of the application's operation. It also reflects the protection status and shows a number of basic functions performed by the application.

If the icon is active  (color), protection is fully enabled or some of its components are running. If the icon is inactive  (black and white), all protection components are disabled.

The Kaspersky PURE icon changes depending on the operation being performed:

-  -- email being scanned;
-  – web traffic being scanned;
-  – databases and application modules update is in progress;
-  - computer should be rebooted to apply updates;
-  – a failure occurred in the operation of some application's component.

The icon also provides access to the basic components of the application interface: context menu (see page 50) and main window (see page 51).

Context menu is opened by right-clicking on the application icon.

To open the Kaspersky PURE main window, left-click on the application icon.

CONTEXT MENU

You can run basic protection tasks from the context menu.

The Kaspersky PURE menu contains the following items:

- **Update** – start the application module and database updates and install updates on your computer.
- **Full Scan** – start a complete scan of your computer for malware objects. Objects residing on all drives, including removable storage media, will be scanned.
- **Virus Scan** – select objects and start a virus scan. By default, the list contains several objects, such as **My documents** folder and mailboxes. You can enlarge the list, select other objects for scan and start virus scan.
- **My Virtual Keyboard** – switch to the virtual keyboard (see page 205).
- **Kaspersky PURE** – open the main application window (see page 51).
- **Settings** – view and configure application settings.
- **Activation** – activate Kaspersky PURE. In order to obtain the status of a registered user, you must activate your application. This menu item is only available if the application has not been activated.
- **About** – display window with information about the application.
- **Pause protection / Resume protection** – temporarily disable or enable the real-time protection components. This menu option does not affect the application's updates, or the execution of virus scans.
- **Pause / Enable My Parental Control** – temporarily disable / enable control of all users. This menu item is only available if the Parental Control component is installed.
- **Block network traffic / Unblock network traffic** – temporarily block / unblock all the computer's network connections.
- **Exit** – close Kaspersky PURE (when this option is selected, the application will be discarded from the computer's RAM).

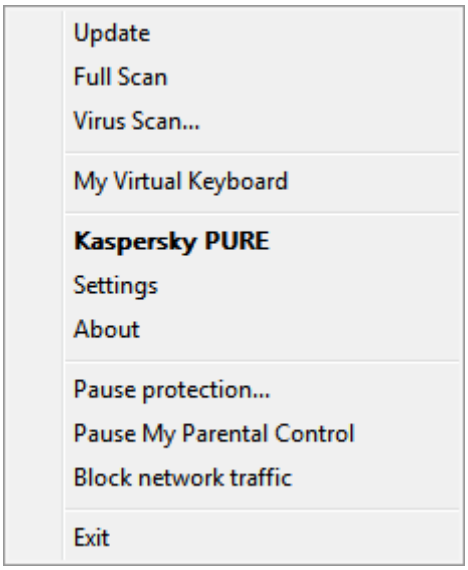


Figure 3. Context menu

If a virus scan task is running at the moment you open the context menu, its name as well as its progress status (percentage complete) will be displayed in the context menu. By selecting the task you can go to the main window containing a report about the current results of its execution.

KASPERSKY PURE MAIN WINDOW

The main application functions are grouped in the main window. The main window can be divided into two parts.

From the top part of the window, you can switch to the main application functions, resume / pause protection, run a virus scan, launch data backup etc. The following main Kaspersky PURE components are located in the top part of the window:

- **My Computer Protection** – comprehensive protection of your computer from any type of threats.
- **My Backup** – creation and storage of backup copies of files that ensure restoration of important data if data loss occurs.
- **My Parental Control** – restriction of the users' access to web resources and applications on the computer, and to instant messaging.

From the lower part of the window, you can switch to additional functions, which secure advanced protection and optimize the system's functioning. In the lower part of the window, in the **Security +** section, the following components and services are grouped:

- **My System Tune-Up** – optimizing the system operation and solving specific computer security tasks.
- **My Virtual Keyboard** – preventing the interception of data entered at the keyboard.
- **My Encryption** – preventing unauthorized access to confidential information.
- **My Password Manager** – protection of personal data, such as passwords, user names, Internet pager accounts, contacts, etc.

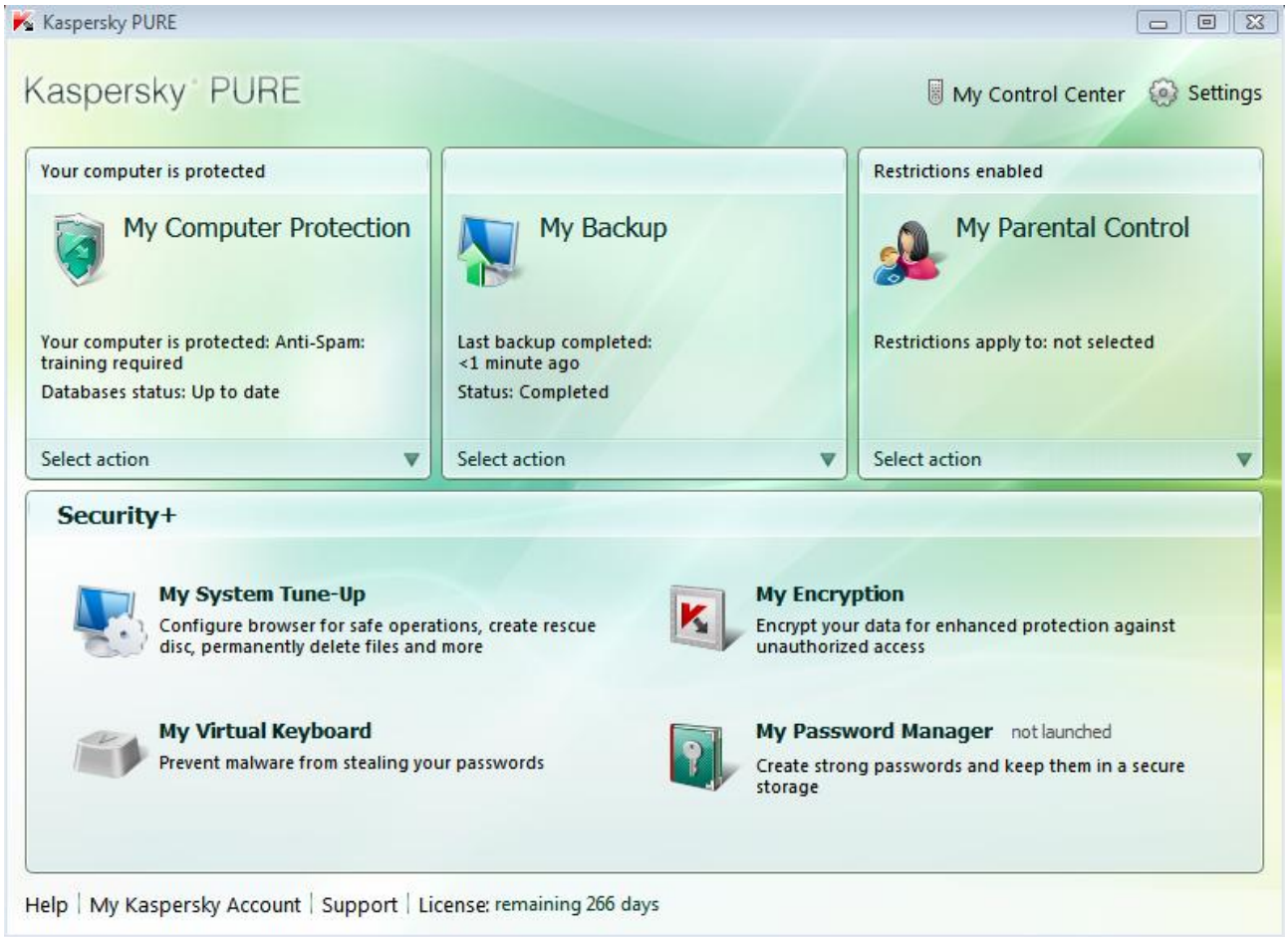


Figure 4. Main application window

You can also use the following buttons and links:

- **My Control Center** – remote administration of Kaspersky PURE (see page 241).

- **Settings** – general application configuration (see page 56).
- **Help** – view Kaspersky PURE help system.
- **My Kaspersky Account** – to enter the user's personal cabinet (https://my.kaspersky.com) at the Technical Support Service's website.
- **Support** – to open the window containing information about the system and links to Kaspersky Lab's information resources (Technical Support service site, forum).
- **License** – Kaspersky PURE activation, and license renewal.

You can change the appearance of Kaspersky PURE by creating and using various graphics and color schemes.

MY COMPUTER PROTECTION

My Computer Protection main window can be divided into three parts:

- The top part of the window indicates your computer's current protection status.

Figure 5. Current status of the computer protection

There are three possible values of protection status: each of them is indicated with a certain color, similar to traffic lights. Green indicates that your computer's protection is at the correct level, while yellow and red colors indicate that there exist various security threats. In addition to malicious programs, threats include obsolete application databases, disabled protection components, the selection of minimum protection settings etc.

Security threats must be eliminated as they appear. For detailed information about threats and how to eliminate them quickly, switch to Security Management Wizard: click the status icon or the panel on which it is located (see fig. above).

- The left part of the window provides quick access to any function of the application, including virus scan tasks, updates, etc.
- The right part of the window contains information about the application function selected in the left part, allows to configure its settings, provides tools for executing virus scan tasks, retrieving updates etc.

You can also use the following links:

- **Settings** – open the application settings window.
- **Quarantine** – start working with quarantined objects.
- **Report** – open the list of events occurred during application operation.
- **Help** – view Kaspersky PURE help system.

BACKUP COPY

The Backup copy main window consists of two parts:

- the left part of the window provides access to the main application functions: to the management of backup tasks and storages of backup copies, and to data restoration;
- the right part of the window contains a list of settings for the function selected in the left part of the window.

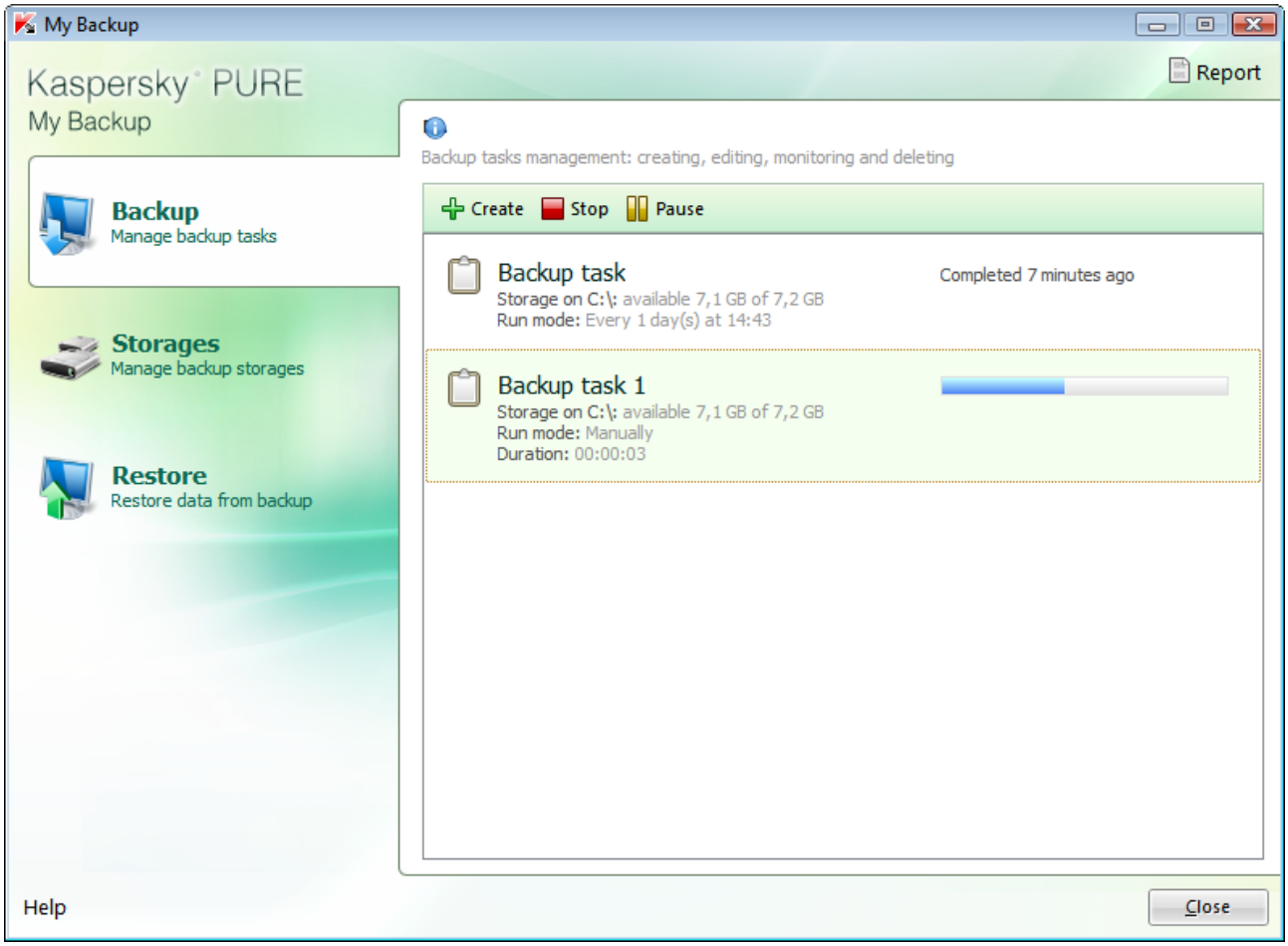


Figure 6. Main window of the Backup module

MY PARENTAL CONTROL

The Parental Control main window consists of two parts:

- the left part of the window provides access to the main functions of the application: custom control configuration and report viewing;

- the right part of the window contains a list of settings for the function selected in the left part of the window.

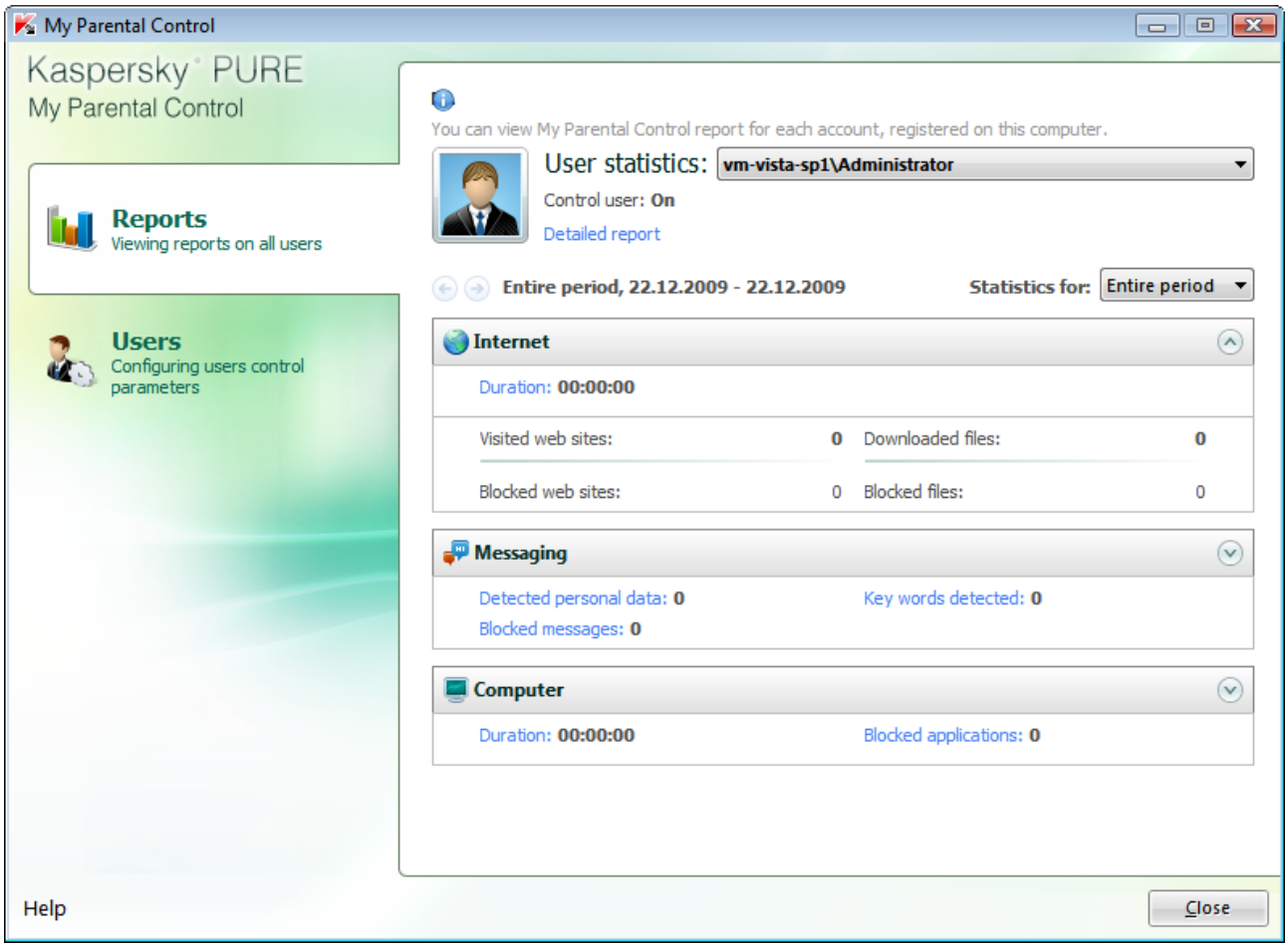


Figure 7. Main window of My Parental Control

NOTIFICATIONS

If events occur during the operation of Kaspersky PURE, special notifications will be displayed on the screen as pop-up messages above the application icon in the Microsoft Windows taskbar.

Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alarm**. A critical event has occurred; for instance, a virus or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. Notifications of this type are highlighted with red.

- **Warning**. A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide on the degree of danger of this event. Notifications of this type are highlighted with yellow.

- **Info**. This notification gives information about non-critical events. This type, for example, includes notifications related to the operation of the Content Filtering component. Information notifications are highlighted in green.

SEE ALSO:

Notifications.....256

APPLICATION SETTINGS WINDOW

Kaspersky PURE settings window may be opened from the main window (see page 51) or from the context menu (see page 50). To open this window, click the **Settings** link in the top part of the main window, or select the appropriate option in the application's context menu.

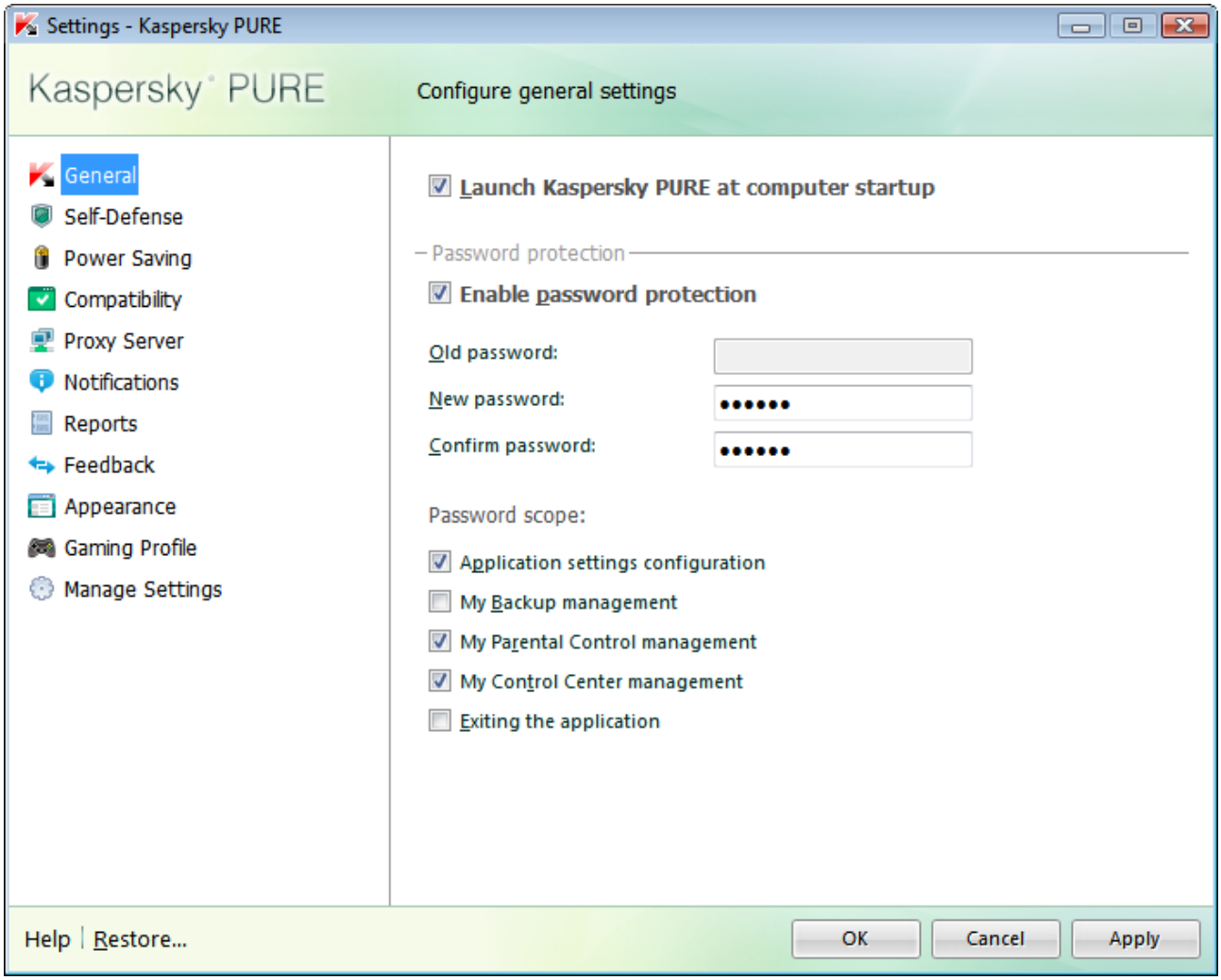


Figure 8. Configuring Kaspersky Anti-Virus

Also, you can configure Computer Protection settings. To do so, click the **My Computer Protection** button in the Kaspersky PURE main window, and in the window that will open, click the **Configure** link in the top part of the window.

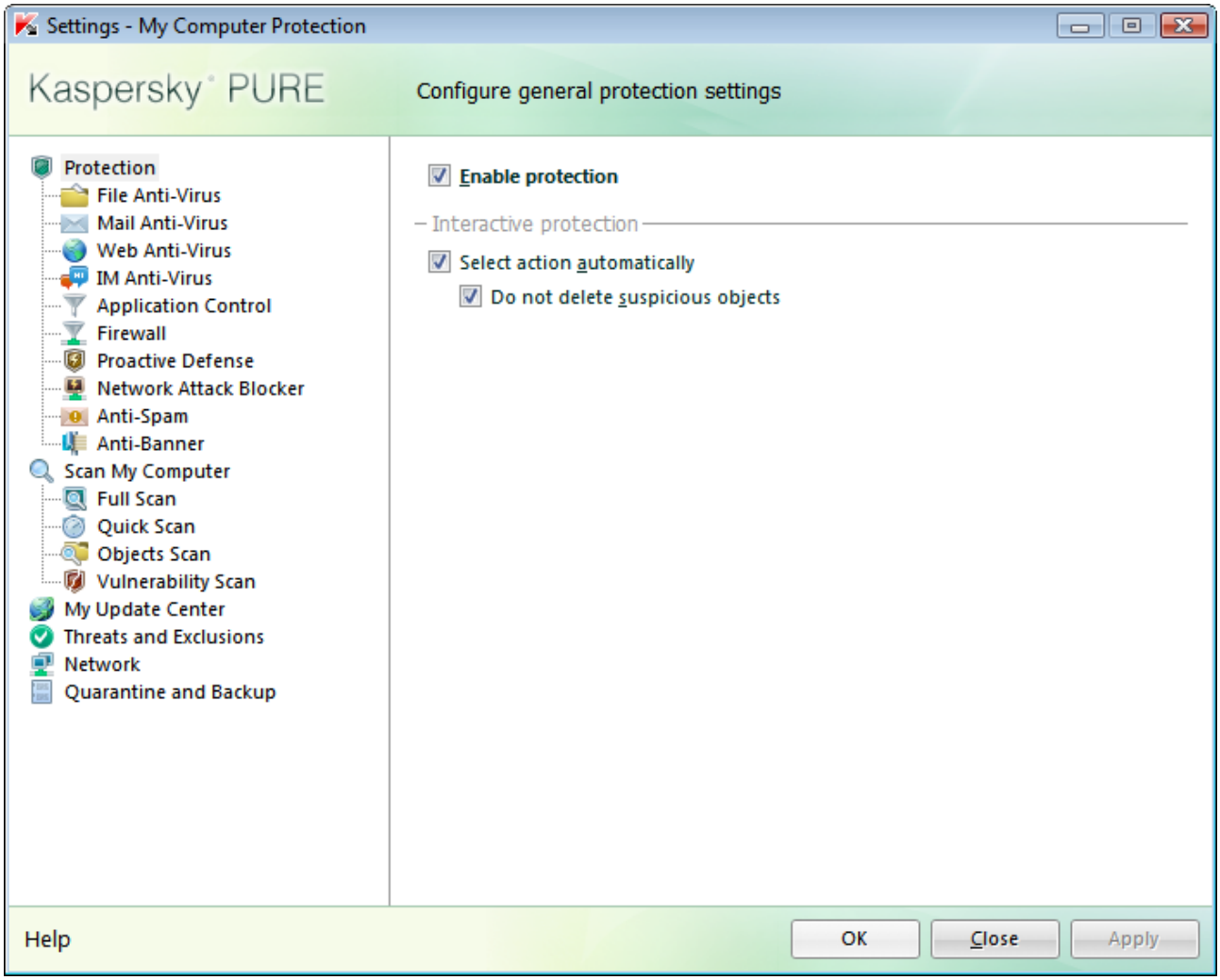


Figure 9. Configuring Kaspersky Anti-Virus

Settings configuration windows consist of two parts:

- the left part of the window provides access to the general tasks and functions of Kaspersky PURE and Computer Protection related to the operation of all components;
- the right part of the window contains a list of settings for the application function, task, etc. selected in the left part of the window.

MY COMPUTER PROTECTION

My Computer Protection components protect your computer against various threats, scan all system objects for viruses and vulnerabilities, and regularly update Kaspersky PURE anti-virus databases and program modules.

IN THIS SECTION:

COMPUTER FILE SYSTEM PROTECTION

File Anti-Virus prevents infection of the computer's file system. It loads when you start your operating system and runs in your computer's RAM, scanning all files that are opened, saved or executed.

By default, File Anti-Virus scans only new or modified files. A collection of settings, called the security level, determines the conditions for file scan. If File Anti-Virus detects a threat, it will perform the assigned action.

File and memory protection level on your computer is determined by the following combinations of settings:

- those creating a protection scope;
- those determining the scan method;
- those determining how compound files are scanned (including scanning of large compound files);
- those determining the scan mode;
- those allowing to pause the component by schedule or during the operation of selected applications.

Kaspersky Lab's specialists advise you not to configure File Anti-Virus settings on your own. In most cases, changing the security level will be enough. To restore the default File Anti-Virus settings, select one of the security levels.

To modify File Anti-Virus settings:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. Make the required changes in the component settings.

IN THIS SECTION:

COMPONENT OPERATION ALGORITHM

The *File Anti-Virus* component loads when you start your operating system and runs in your computer's memory, scanning all files that are opened, saved, or executed.

By default, File Anti-Virus only scans new or modified files; in other words, files that have been added or modified since the previous scan. Files are scanned according to the following algorithm:

1. The component intercepts every attempt by the user or by any program to access any file.

2. File Anti-Virus scans iChecker and iSwift databases for information about the intercepted file, and determines if it should scan the file, based on the information retrieved.

The following operations are performed when scanning:

1. The file is scanned for viruses. Malicious objects are recognized based on My Computer Protection databases. The database contains descriptions of all malicious programs and threats currently known, and methods for processing them.

2. After the analysis you have the following available courses of action for My Computer Protection:

    a. If malicious code is detected in the file, File Anti-Virus blocks the file, creates a backup copy and attempts to perform disinfection. If the file is successfully disinfected, it becomes available again. If disinfection fails, the file is deleted.

    b. If potentially malicious code is detected in the file (but the maliciousness is not absolutely guaranteed), the file proceeds to disinfection and then is sent to the special storage area called Quarantine.

    c. If no malicious code is discovered in the file, it is immediately restored.

The application will notify you when an infected or a possibly infected file is detected. If an infected or potentially infected object is detected, a notification with a request for further actions will be displayed onscreen. You will be offered the following:

- quarantine the object, allowing the new threat to be scanned and processed later using updated databases;
- delete the object;
- skip the object if you are absolutely sure that it is not malicious.

CHANGING SECURITY LEVEL OF FILES AND MEMORY

The security level is defined as a preset configuration of the File Anti-Virus component settings. Kaspersky Lab specialists distinguish three security levels. The decision of which level to select should be made by the user based on the operational conditions and the current situation. You will be offered to select one of the following options for security level:

- **High**. Set this level if you suspect that your computer has a high chance of being infected.
- **Recommended**. This level provides an optimum balance between the efficiency and security and is suitable for most cases.
- **Low**. If you work in a protected environment (for example, in a corporate network with centralized security management), the low security level may be suitable. The low security level can also be set if you are working with resource-consuming applications.

Before enabling the low security level, it is recommended to perform the full scan of computer at high security level.

If none of the preset levels meet your needs, you can configure the File Anti-Virus's settings (see section "Computer file system protection" on page 59) on your own. As a result, the security level's name will be changed to **Custom**. To restore the default component's settings, select one of the preset security levels.

To change the current file and memory security level, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Set the required security level for the component you have selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

Based on the scan results, File Anti-Virus assigns one of the following statuses to the objects detected:

- malicious program (such as, a *virus* or a *Trojan*);
- *potentially infected* status when the scan cannot determine if the object is infected. This means that the application detected a sequence of code in the file from an unknown virus, or modified code from a known virus.

If Computer Protection detects infected or potentially infected objects when scanning for viruses, it will notify you about it. You should respond to the threat by selecting an action on the object. Computer Protection selects the **Prompt for action** option as the action on a detected object which is the default setting. You can change the action. For example, if you are sure that each detected object should be attempted to disinfect, and do not want to select the **Disinfect** action each time you receive a notice about the detection of an infected or suspicious object, you should select the following action: **Do not prompt. Disinfect**.

Before attempting to disinfect or delete an infected object, Computer Protection creates a backup copy of it to allow later restoration or disinfection.

If you work in automatic mode (see section "Step 3. Selecting protection mode" on page 41), Computer Protection will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Skip**.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Specify the required action for the component you have selected.

CREATING A PROTECTION SCOPE

A protection scope should be understood not only as the location of the objects to be scanned, but also the type of files to be scanned. By default, Computer Protection only scans potentially infectible files run from any hard drive, network drive, or removable medium.

You can expand or narrow down the protection scope by adding / removing objects to be scanned, or by changing the type of files to be scanned. For example, you wish to scan only *exe* files run from network drives. However, you should make sure that you will not expose your computer to the threat of infection when narrowing down the protection scope.

When selecting file types you should remember the following:

- Some file formats (e.g., *txt*) have a low risk of containing malicious code which could subsequently be activated. At the same time, there are formats that contain or may contain an executable code (*exe*, *dll*, *doc*). The risk of activating malicious code in such files is quite high.
- The intruder can send a virus to your computer with the extension *txt*, which could be an executable file renamed as *txt* file. If you have selected the **Files scanned by extension** option, such a file will be skipped by the scan. If the **Files scanned by format** setting has been selected, then, regardless of the extension, File Anti-Virus will analyze the file header, uncover that the file is an *.exe* file, and scan it for viruses.

To edit the object scan list:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **General** tab, in the **Protection scope** section, click the **Add** link.
6. In the **Select object to scan** window, select an object and click the **Add** button.
7. After you have added all required objects, click the **OK** button in the **Select object to scan** window.
8. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

To change the type of scanned objects:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **General** tab, in the **File types** block, select the required parameter.

USING HEURISTIC ANALYSIS

Objects are scanned using databases which contain descriptions of all known malware and the corresponding disinfection methods. Computer Protection compares each scanned object with the database records to determine accurately if the object is malicious, and if so, into which class of malware it falls. This approach is called *signature analysis* and is always used by default.

Since new malicious objects appear daily, there is always some malware which are not described in the databases, and which can only be detected using heuristic analysis. This method presumes the analysis of the actions an object performs within the system. If those actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious. This allows new threats to be detected even before they have been researched by virus analysts.

If a malicious object is detected, you will receive a notification prompting for action.

Additionally you can set the detail level for scans. It sets the balance between the thoroughness of searches for new threats, the load on the operating system's resources and the time required for scanning. The higher the detail level, the more resources the scan will require, and the longer it will take.

- *To use the heuristic analysis, and set the detail level for scans:*

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Performance** tab, in the **Scan methods** block, check the **Heuristic analysis** box and specify the detail level for the scan.

SCAN OPTIMIZATION

To shorten the duration of scans and increase the operating speed of Computer Protection, you can opt to scan only new files and files modified since the last scan. This mode extends to simple and compound files.

- *To scan only new files and files which have altered since their last scan:*

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Performance** tab, in the **Scan optimization** block, check the **Scan only new and changed files** box.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden this way a compound file should be unpacked, which can significantly lower the scan speed.

Installer packages and files containing OLE objects are executed when they are opened, which makes them more dangerous than archives. By disabling archive scans and enabling scans for these file types, you can protect your computer against execution of malicious code and, at the same time, increase the scan speed.

By default, Computer Protection scans only embedded OLE objects.

To modify the list of scanned compound files:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Performance** tab, in the **Scan of compound files** block, check the boxes for the types of compound files to be scanned by the application.

SCANNING LARGE COMPOUND FILES

When large compound files are scanned, their preliminary unpacking may require a long time. This term may be reduced if files are scanned in the background. If a malicious object is detected while working with such a file, Computer Protection will notify you about it.

To reduce the delay when accessing compound files, one may disable unpacking the files of a size, which is larger than the specified value. When files are extracted from an archive, they will always be scanned.

For Computer Protection to unpack large-sized files in the background:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Performance** tab, in the **Scan of compound files** block, click the **Additional** button.
6. In the **Compound files** window, check the **Extract compound files in the background** box and specify the minimum file size in the field below.

To prevent Computer Protection from unpacking large-sized compound files:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Performance** tab, in the **Scan of compound files** block, click the **Additional** button.

6. In the **Compound files** window that will open, check the **Do not unpack large compound files** box and specify the file size in the field next to it.

CHANGING THE SCAN MODE

The scan mode is the condition, which triggers File Anti-Virus into activity. By default, Computer Protection uses smart mode, which determines if the object is subject to scan, based on the actions performed on it. For example, when working with a Microsoft Office document, Computer Protection scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

You can change the object scan mode. The scan mode should be selected depending on the files you work with most of the time.

To change the object scan mode:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Additional** tab, in the **Scan mode** block, select the required mode.

SCAN TECHNOLOGY

Additionally you can specify which technologies will be used by the File Anti-Virus component:

- **iChecker**. This technology can increase scan speed by excluding certain objects from the scan. An object is excluded from the scan with a special algorithm that uses the release date of Computer Protection databases, the date the object was last scanned, and any modifications to the scan settings.

  For example, you have an archive file with the *not infected* status assigned after the scan. The next time the application will exclude this archive from the scan unless it has been altered or the scan settings have been changed. If the archive's structure has changed because a new object had been added to it, or if the scan settings have changed, or if the application databases have been updated, then the application will re-scan the archive.

  There are limitations to iChecker: it does not work with large files and applies only to the objects with a structure that the application recognizes (for example, *.exe*, *.dll*, *.lnk*, *.ttf*, *.inf*, *.sys*, *.com*, *.chm*, *.zip*, *.rar*).

- **iSwift**. This technology is a development of the iChecker technology for computers using an NTFS file system. There are limitations to iSwift: it is bound to a specific file location in the file system and can apply only to objects in NTFS.

To change the object scan technology:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Additional** tab, in the **Scan technologies** block, select the required setting value.

PAUSING THE COMPONENT: CREATING A SCHEDULE

When certain programs which require considerable computer resources are in progress, you can temporarily pause the operation of the File Anti-Virus component, which allows quicker access to objects. To decrease the load and ensure quick access to objects, you can set a schedule for disabling the component.

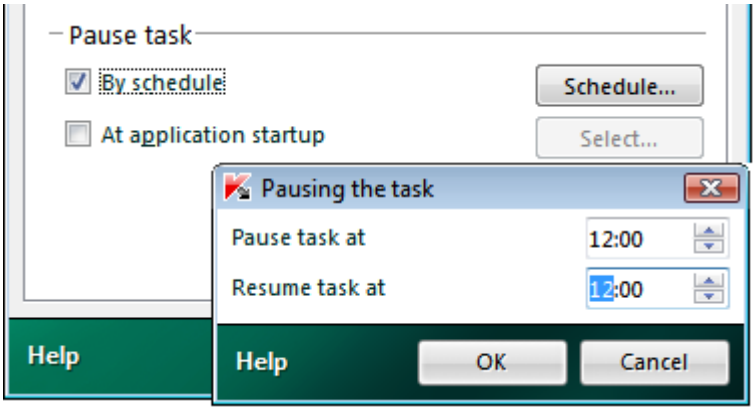


Figure 10. Creating a schedule

To configure a schedule for pausing the component:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Additional** tab, in the **Pause task** block, check the **By schedule** box and click the **Schedule** button.
6. In the **Pausing the task** window, specify the time period (in 24-hour HH:MM format) for which protection will be paused (**Pause task at** and **Resume task at** fields).

PAUSING THE COMPONENT: CREATING AN APPLICATIONS LIST

When certain programs which require considerable computer resources are in progress, you can temporarily pause the operation of the File Anti-Virus component, which allows quicker access to objects. To decrease the load and ensure quick access to objects, you can configure the settings for disabling the component when working with certain applications.

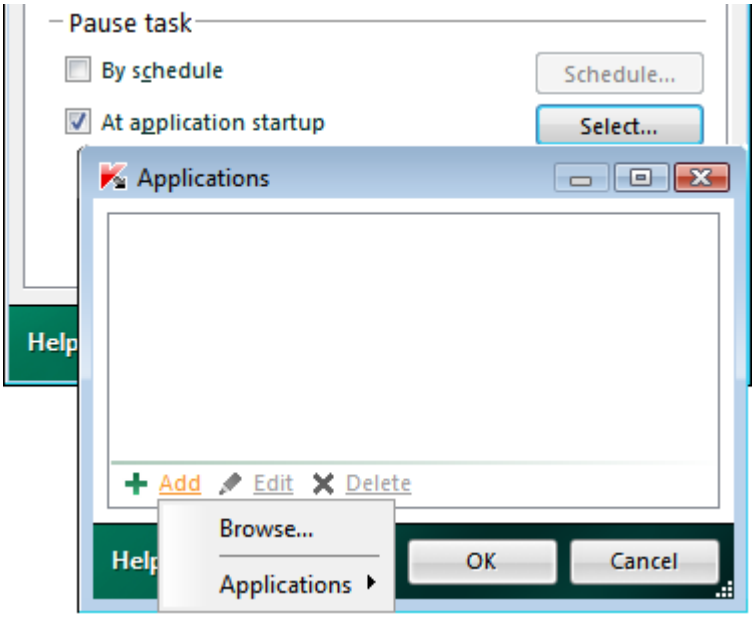


Figure 11. Creating application list

Configuring the disabling of File Anti-Virus component if it conflicts with certain applications is an emergency measure! If any conflicts arouse when working with the component, please contact Kaspersky Lab's Technical Support Service (http://support.kaspersky.com). The support specialists will help you resolve simultaneous operation of Computer Protection with the software on your computer.

To configure pausing the component while specified applications are being used, perform the following actions:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Additional** tab, in the **Pause task** block, check the **At application startup** box and click the **Select** button.
6. In the **Applications** window, create a list of applications which will pause the component when running.

RESTORING DEFAULT PROTECTION SETTINGS

When configuring File Anti-Virus, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default protection settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **File Anti-Virus** component.
4. In the **Security level** section, click the **Default level** button for the component selected.

MAIL PROTECTION

Mail Anti-Virus scans incoming and outgoing messages for the presence of malicious objects. It is launched when the operating system loads, is located in computer RAM and scans all email messages received via the POP3, SMTP, IMAP, MAPI and NNTP protocols.

A collection of settings called the security level, determines the way of scanning the email. Once a threat is detected, Mail Anti-Virus performs the action you have specified (see section "Changing actions to be performed on detected objects" on page 71). The rules with which your email is scanned are defined by a collection of settings. They can be divided into groups, determining the following features:

- from the protected mail stream;
- of using the methods of heuristic analysis;
- of scanning the compound files;
- of filtering the attached files.

Kaspersky Lab advises you not to configure Mail Anti-Virus settings on your own. In the majority of cases, selecting a different security level is sufficient. You can restore default settings of Mail Anti-Virus. To do so, select one of the security levels.

To edit Mail Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. Make the required changes in the component settings.

IN THIS SECTION:

COMPONENT OPERATION ALGORITHM

Computer Protection includes the component, which ensures scanning the email for dangerous objects, named *Mail Anti-Virus*. It loads when the operating system launches and runs continually, scanning all email on the POP3, SMTP, IMAP, MAPI and NNTP protocols, as well as on secure connections (SSL) for POP3 and IMAP.

The indicator of the component's operation is the application icon in the taskbar notification area, which looks like  whenever an email message is being scanned.

By default, email protection is carried out as follows:

1. Each email received or sent by the user is intercepted by the component.

2. The email is broken down into its parts: the email heading, its body, and attachments.

3. The body and attachments of the email message (including OLE objects) are scanned for dangerous objects. Malicious objects are detected with the databases used by Computer Protection, and with the heuristic algorithm. The database contains descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the database.

4. After the virus scan, the following behavior options are available:

    - If the body or attachments of the email contain malicious code, the File Anti-Virus component will block the email, create a backup copy of it and attempt to disinfect the object. After the email message is successfully disinfected, it returns to the user. If the disinfection fails, the infected object will be deleted from the message. After the virus scan, special text is inserted in the subject line of the email, notifying you that the email has been processed by Computer Protection.

    - If potentially malicious code is detected in the body or an attachment (but the maliciousness is not absolutely guaranteed), the suspicious part of the email will be placed to the special storage area called Quarantine.

    - If no malicious code is discovered in the email, it is immediately made available again to the user.

An integrated extension module is provided for Microsoft Office Outlook (see section "Email scanning in Microsoft Office Outlook" on page 72) that allows for fine-tuning the email client.

If you are using The Bat!, Computer Protection can be used in conjunction with other anti-virus applications. At that, the email traffic processing rules (see section "Email scanning in The Bat!" on page 72) are configured directly in The Bat! and override the application's email protection settings.

When working with other mail programs, including Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora, and Incredimail, the Mail Anti-Virus component scans email on SMTP, POP3, IMAP, and NNTP protocols.

Note that when working with Thunderbird mail client, email messages transferred via IMAP will not be scanned for viruses if any filters moving messages from the **Inbox** folder are used.

CHANGING EMAIL PROTECTION SECURITY LEVEL

The security level is defined as a preset configuration of File Anti-Virus settings. Kaspersky Lab specialists distinguish three security levels. The decision of which level to select should be made by the user based on the operational conditions and the current situation. You may select one of the following security levels:

- **High**. If you work in a non-secure environment, the maximum security level will suit you the best. An example of such environment is a connection to a free email service, from a network that is not guarded by centralized email protection.

- **Recommended**. This level provides an optimum balance between the efficiency and security and is suitable for most cases. This is also the default setting.

- **Low**. If you work in a well secured environment, low security level can be used. An example of such an environment might be a corporate network with centralized email security.

If none of the preset levels meet your needs, you can configure the Mail Anti-Virus's settings (see section "Mail protection" on page 69) on your own. As a result, the security level's name will be changed to **Custom**. To restore the default component's settings, select one of the preset security levels.

To change the preset email security level:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
4. Set the required security level for the component you have selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

Mail Anti-Virus scans an email message. If the scan indicates that the email or any of its parts (body, attachment) is infected or potentially infected, the component's further actions depend on the status of the object and the action selected.

As a result of scanning, Mail Anti-Virus assigns one of the following statuses to detected objects:

- malicious program (such as, a *virus* or a *Trojan*).
- *potentially infected* status when the scan cannot determine if the object is infected. This means that the email or attachment contains a sequence of code from an unknown virus, or modified code from a known virus.

If Computer Protection detects infected or potentially infected objects when scanning the email, it will notify you about them. You should respond to the threat by selecting an action on the object. Computer Protection selects the **Prompt for action** option as the action on a detected object which is the default setting. You can change the action. For example, if you are sure that each detected object should be attempted to disinfect and do not want to select the **Disinfect** action each time you receive a notice about the detection of an infected or suspicious object in a message, you should select the following action: **Do not prompt. Disinfect**.

Before attempting to disinfect or delete an infected object, Computer Protection creates a backup copy of it to allow later restoration or disinfection.

If you work in automatic mode (see section "Step 3. Selecting protection mode" on page 41), Computer Protection will automatically apply the action recommended by Kaspersky Lab specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Skip**.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
4. Specify the required action for the component you have selected.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Computer Protection scans both incoming and outgoing messages. If you have selected the scanning of incoming messages only, you are advised to

scan outgoing mail when you first begin using My Computer Protection, because it is likely that there are worms on your computer which will propagate themselves via email. This will avoid unpleasant situations caused by unmonitored mass emailing of infected emails from your computer.

The protection scope also includes the settings used to integrate the Mail Anti-Virus component into the system, and the protocols to be scanned. By default, the Mail Anti-Virus component is integrated into the Microsoft Office Outlook and The Bat! email client applications.

- *To disable scans of outgoing emails, please do the following:*

  1. Open the main application window and click the **My Computer Protection** button.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
  4. Click the **Settings** button for the component you have selected.
  5. In the window that will open, on the **General** tab, in the **Protection scope** block, specify the required values for the settings.

- *To select the protocols to scan and the settings to integrate Mail Anti-Virus into the system, please do the following:*

  1. Open the main application window and click the **My Computer Protection**.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
  4. Click the **Settings** button for the component you have selected.
  5. In the window that will open, on the **Additional** tab, in the **Connectivity** block, select the required settings.

EMAIL SCANNING IN MICROSOFT OFFICE OUTLOOK

If you use Microsoft Office Outlook as the mail client, you may configure additional settings for scanning your mail for viruses.

A special plug-in is installed in Microsoft Office Outlook when you install Computer Protection. It allows you to configure Mail Anti-Virus settings quickly, and determine when email messages will be scanned for dangerous objects.

The plug-in comes in the form of a special **Email protection** tab located in the **Tools** → **Options** menu. On the tab you can specify the email scan modes.

- *To specify complex filtering conditions:*

  1. Openthe main Microsoft Outlook window.
  2. Select **Tools** → **Options** from the application menu.
  3. On the **Email protection** tab specify the required email scan mode.

EMAIL SCANNING IN THE BAT!

Actions on infected email objects in The Bat! are defined using the application's own tools.

Mail Anti-Virus settings determining if incoming and outgoing messages should be scanned, which actions should be performed on dangerous objects in email, and which exclusions should apply, are ignored. The only thing that The Bat! takes into account is scanning of attached archives.

The email protection settings extend to all the anti-virus modules installed on the computer that support work with the Bat!.

Please remember, incoming email messages are first scanned by Mail Anti-Virus and only after that – by The Bat! mail client plug-in. If a malicious object is detected, Computer Protection will inform you of this without fail. If you select the **Disinfect** (**Delete**) action in the notification window of Mail Anti-Virus, actions aimed at eliminating the threat will be performed by Mail Anti-Virus. If you select the **Skip** action in the notification window, the object will be disinfected by The Bat! plug-in. When sending email messages, the scan is first performed by the plug-in, then by Mail Anti-Virus.

You must decide:

- Which stream of email messages will be scanned (incoming, outgoing).
- At what point in time email objects will be scanned (when opening an email message or before it is saved to the disk).
- The actions taken by the mail client when dangerous objects are detected in emails. For example, you could select:
  - **Attempt to disinfect infected parts** – if this option is selected, the infected object will be attempted to disinfect; if it cannot be disinfected, the object will remain in the message.
  - **Delete infected parts** – if this option is selected, the dangerous object in the message will be deleted regardless of whether it is infected or suspected to be infected.

By default, The Bat! places all infected email objects in Quarantine without attempting to disinfect them.

The Bat! does not give special headers to emails containing dangerous objects.

To set up email protection rules in The Bat!:

1. Open the main The Bat! window.
2. Select the **Settings** item from the **Properties** menu of the mail client.
3. Select the **Virus protection** item from the settings tree.

USING HEURISTIC ANALYSIS

Essentially, the heuristic method analyzes the object's activities in the system. If those actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious. This allows new threats to be detected before they have been analyzed by virus analysts. By default, heuristic analysis is enabled.

Computer Protection will notify you when a malicious object is detected in a message. You should react to the notification by further processing the message.

Additionally you can set the detail level for scans: **Light**, **Medium**, or **Deep**. To do so, move the slider bar to the selected position.

To enable/disable the heuristic analysis, and to set the detail level for the scan, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **General** tab, in the **Scan methods** block, check / uncheck the **Heuristic analysis** box and specify the detail level for the scan.

SCAN OF COMPOUND FILES

The selection of compound files scan mode affects the performance of Computer Protection. You can enable or disable the scan of attached archives and limit the maximum size of archives to be scanned.

To configure the settings for the scan of compound files:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **General** tab, select the scan mode of compound files.

ATTACHMENT FILTERING

You can configure filtration conditions for email attachments. Using the filter will add to your computer's security since malicious programs spread via email are most frequently sent as attachments. By renaming or deleting certain attachment types, you can protect your computer against potential hazards, such as automatically opening attachments when a message is received.

If your computer is not protected by any local network software (you access the Internet directly without a proxy server or a firewall), you are advised not to disable scanning of attached archives.

To configure attachment filtering settings:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Attachment filter** tab, specify the filtering conditions for email attachments. When you select either of the last two modes, the list of file types will become enabled in which you can specify the required types or add a mask to select a new type.

   If you need to add a mask of a new type, click the **Add** link and enter the required data in the **Input file name mask** window that will open.

RESTORING DEFAULT MAIL PROTECTION SETTINGS

When configuring Mail Anti-Virus, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default mail protection settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Mail Anti-Virus** component.

4. In the **Security level** section, click the **Default level** button for the component selected.

WEB TRAFFIC PROTECTION

Whenever you use the Internet, you subject information stored on your computer to the risk of infection by dangerous programs. These can infiltrate your computer while you are downloading free software, or browsing knowingly safe sites, which have recently suffered network attacks. Moreover, network worms can penetrate your computer before you open a webpage or download a file just because your computer is connected to the Internet.

The *Web Anti-Virus* component is designed to ensure the security while using the Internet. It protects your computer against data coming into your computer via the HTTP protocol, and also prevents dangerous scripts from being executed on the computer.

Web protection monitors HTTP traffic that passes only through the ports included in the monitored port list. A list of ports that are most commonly used for transmitting email and HTTP traffic is included in the My Computer Protection installation package. If you use ports that are not on this list, you must add them to the list to protect traffic using these ports.

If you work in a non-secure area, you are recommended to use Web Anti-Virus while working in the Internet. If your computer is running on a network protected by a firewall of HTTP traffic filters, Web Anti-Virus provides additional security when using the Internet.

A collection of settings, called the security level, determines the way of scanning the traffic. If Web Anti-Virus detects a threat, it will perform the assigned action.

Your web protection level is determined by a group of settings. The settings can be broken down into the following groups:

- protection scope settings;
- settings that determine the efficiency of traffic protection (using heuristic analysis, scan optimization).

Kaspersky Lab advises you not to configure Web Anti-Virus component settings on your own. In the majority of cases, selecting a different security level is sufficient.

To edit Web Anti-Virus settings:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. Make the required changes in the component settings.

IN THIS SECTION:

COMPONENT OPERATION ALGORITHM

Web Anti-Virus protects your computer against data coming onto the computer via HTTP, and prevents hazardous scripts from running on the computer.

This section discusses the component's operation in more detail. HTTP traffic is protected using the following algorithm:

1. Each web page or file that is accessed by the user, or by a program via the HTTP protocol, is intercepted and analyzed for malicious code by Web Anti-Virus. Malicious objects are detected using both Computer Protection databases and the heuristic algorithm. The database contains descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the database.

2. After the analysis, you have the following available courses of action:

   - If a web page or an object accessed by the user contains malicious code, access to them is blocked. A notification is displayed that the object or page being requested is infected.

   - If the file or web page does not contain malicious code, the program immediately grants the user access to it.

Scripts are scanned according to the following algorithm:

1. Each script run on a web page is intercepted by Web Anti-Virus and is analyzed for malicious code.

2. If the script contains malicious code, Web Anti-Virus blocks it and informs the user of it with a special pop-up message.

3. If no malicious code is discovered in the script, it is run.

Scripts are intercepted only on the web pages, opened in Microsoft Internet Explorer.

CHANGING HTTP TRAFFIC SECURITY LEVEL

The security level is defined as a preset configuration of File Anti-Virus settings. Kaspersky Lab specialists distinguish three security levels. The decision of which level to select should be made by the user based on the operational conditions and the current situation. You will be offered to select one of the following options for security level:

- **High**. This security level is recommended for sensitive environments when no other HTTP security tools are being used.
- **Recommended**. This security level is optimal for using in most situations.
- **Low**. Use this security level if you have additional HTTP traffic protection tools installed on your computer.

If none of the preset levels meet your needs, you can configure the Web Anti-Virus's settings (see section "Web traffic protection" on page 76) on your own. As a result, the security level's name will be changed to **Custom**. To restore the default component's settings, select one of the preset security levels.

To change the preset security level for web traffic:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. Set the required security level for the component you have selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

Once analysis of an HTTP object shows that it contains malicious code, the response by the Web Anti-Virus component depends on the action you have selected.

Web Anti-Virus always blocks actions by dangerous objects and issues pop-up messages that inform the user of the action taken. The action on a dangerous script cannot be changed – the only available modification is disabling script scan module (see section "Selecting the scan type" on page 79).

If you work in automatic mode (see section "Step 3. Selecting protection mode" on page 41), Computer Protection will automatically apply the action recommended by Kaspersky Lab's specialists when dangerous objects are detected.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. Specify the required action for the component you have selected.

CREATING A PROTECTION SCOPE

Creating a protection scope means selecting the type of scan (see section "Selecting the scan type" on page 79) of objects by Web Anti-Virus, and creating the list of trusted web addresses, which contain information not subject to scan for dangerous objects by the component.

You can create a list of trusted web addresses whose content you unconditionally trust. Web Anti-Virus will not analyze data from those addresses for dangerous objects. This option may be useful, for instance, when Web Anti-Virus interferes with downloading a particular file.

To create the list of trusted web addresses, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the **Web Anti-Virus** window that will open, in the **Scan optimization** block, check the **Do not scan HTTP traffic from trusted web addresses** box and click the **Select** button.
6. In the **List of trusted web addresses** window that will open, click the **Add** link.
7. In the **Address mask (URL)** window that will open, enter a trusted web address (or a mask for trusted address).

SELECTING THE SCAN TYPE

The protection scope creation task (see page 78), along with creation of the trusted web addresses list, also includes the selection of traffic scan type performed by Web Anti-Virus. By type, the scan is divided into script scan and HTTP traffic scan.

By default, Web Anti-Virus scans HTTP traffic and scripts simultaneously.

HTTP traffic scan includes not only virus scan but also checking links to know if they are included in the list of suspicious web addresses and / or in the list of phishing web addresses.

Checking the links if they are included in the list of phishing web addresses allows to avoid phishing attacks, which, as a rule, look like email messages from would-be financial institutions and contain links to their websites. The message text convinces the reader to click the link and enter confidential information in the window that follows, for example, a credit card number or a login and password for an Internet banking site where financial operations can be carried out.

Since the link to a phishing site may be received not only in an email message but in any other way, for example, in the text of an ICQ message, Web Anti-Virus component traces the attempts of accessing a phishing site at the level of HTTP traffic scan, and blocks them.

Checking the links if they are included in the list of suspicious web addresses allows to track web sites included in the black list. The list is created by Kaspersky Lab's specialists and is part of the application installation package.

In order for Web Anti-Virus to scan scripts, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the **Web Anti-Virus** window that will open, in the **Additional** block, make sure that the **Block dangerous scripts in Microsoft Internet Explorer** box is checked. Web Anti-Virus will scan all scripts processed in Microsoft Internet Explorer, as well as any other WSH scripts (JavaScript, Visual Basic Script, etc.) launched when the user works on the computer.

   Additionally you can use the Kaspersky URL Advisor (see page 80). To do so, check the **Mark phishing and suspicious URLs in Microsoft Internet Explorer and Mozilla Firefox** box. Web Anti-Virus will mark phishing and suspicious URLs to web addresses detected in browsers (Microsoft Internet Explorer and Mozilla Firefox).

To scan links using the base of suspicious web addresses and / or phishing web addresses, please do the following:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. Click the **Settings** button for the component you have selected.
5. In the **Web Anti-Virus** window that will open, in the **Scan methods** block, make sure that the **Check if URLs are listed in the base of suspicious web addresses** and / or **Check if URLs are listed in the base of phishing web addresses** boxes are checked.

KASPERSKY URL ADVISOR

Computer Protection includes the URL scanning module managed by Web Anti-Virus. This module checks if links located on the web page belong to the list of suspicious and phishing web addresses. You can create a list of trusted web addresses the content of which should not be scanned, and a list of web addresses the content of which should be scanned without fail. This module is built in Microsoft Internet Explorer and Mozilla Firefox browsers as a plug-in.

To enable the URL scanning module, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. In the **Security level** section, click the **Settings** button for the component selected.
5. In the **Web Anti-Virus** window that will open, in the **Additional** block, check the **Mark phishing and suspicious URLs in Microsoft Internet Explorer and Mozilla Firefox** box.

To create the list of trusted web addresses, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. In the **Security level** section, click the **Settings** button for the component selected.
5. In the **Web Anti-Virus** window that will open, in the **Additional** block, click the **Settings** button.
6. In the **Kaspersky URL Advisor** window that will open, select the **On all web pages** option and click the **Exclusions** button.
7. In the **List of trusted web addresses** window that will open, click the **Add** link.
8. In the **Address mask (URL)** window that will open, enter a trusted web address (or a mask for trusted address).

To create the list of websites which content should be scanned:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. In the **Security level** section, click the **Settings** button for the component selected.
5. In the **Web Anti-Virus** window that will open, in the **Additional** block, click the **Settings** button.

6. In the **Kaspersky URL Advisor** window that will open, select the **On the selected web pages** option and click the **Select** button.

7. In the **List of checked web addresses** window that will open, click the **Add** link.

8. In the **Address mask (URL)** window that will open, enter a web address (or a mask of it).

USING HEURISTIC ANALYSIS

Essentially, the heuristic method analyzes the object's activities in the system. If those actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious. This allows new threats to be detected even before they have been researched by virus analysts. By default, heuristic analysis is enabled.

Computer Protection will notify you when a malicious object is detected in a message. You should react to the notification by further processing the message.

Additionally you can set the detail level of scanning: **Light**, **Medium**, or **Deep**. To do so, move the slider bar to the selected position.

To enable/disable the heuristic analysis, and to set the detail level for the scan, please do the following:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.

4. Click the **Settings** button for the component you have selected.

5. In the **Web Anti-Virus** window that will open, in the **Scan methods** block, check / uncheck the **Heuristic analysis** box and specify the scan detail level below.

SCAN OPTIMIZATION

To detect malicious code more efficiently, Web Anti-Virus buffers fragments of objects downloaded from the Internet. When using this method, Web Anti-Virus only scans an object after it has been completely downloaded. Then, the object is scanned for viruses and returned to the user for work or blocked, depending on scan results.

However, buffering objects increases object processing time, and hence the time before the application returns objects to the user. This can cause problems when copying and processing large objects because the connection with the HTTP client may time out.

To solve this problem, we suggest limiting the buffering time for web object fragments downloaded from the Internet. When this time limit expires, the user will receive the downloaded part of the file without scanning, and once the object is fully copied, it will be scanned in its entirety. This allows reducing the time period needed to transfer the object to the user, and eliminating the problem of disconnection; at that, security level for Internet use will not reduce.

By default, the buffering time for file fragments is limited to one second. Increasing this value or removing the buffering time limit will result in better virus scans but somewhat slower access to the object.

To set a time limit for fragment buffering or remove it, please do the following:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.

4. Click the **Settings** button for the component you have selected.

5. In the **Web Anti-Virus** window that will open, in the **Scan optimization** block, check / uncheck the **Limit fragment buffering time** box and enter the time value (in seconds) in the field right to it.

RESTORING DEFAULT WEB PROTECTION SETTINGS

When configuring Web Anti-Virus, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default Web Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Web Anti-Virus** component.
4. In the **Security level** section, click the **Default level** button for the component selected.

PROTECTING INSTANT MESSENGERS TRAFFIC

Besides the additional features for comfortable Internet surfing, instant messaging clients (further referred to as *IM clients*), which have widely spread nowadays, have caused potential threats to computer security. Messages that contain URLs to suspicious websites and those used by intruders for phishing attacks may be transferred using IM clients. Malicious programs use IM clients to send spam messages and URLs to the programs (or the programs themselves), which steal users' ID numbers and passwords.

The *IM Anti-Virus* component is designed to ensure safe operation of IM clients. It protects the information that comes to your computer via IM protocols.

The product ensures safe operation of various applications for instant messaging, including ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent and IRC.

The Yahoo! Messenger and Google Talk applications use the SSL protocol. In order for IM Anti-Virus to scan the traffic of these applications, it is necessary to use the encrypted connections scan (see page 170). To do so, check the **Scan encrypted connections** box in the **Network** section.

Traffic is scanned based on a certain combination of settings. If threats are detected in a message, IM Anti-Virus substitutes this message with a warning message for the user.

Your IM traffic protection level is determined by a group of settings. The settings can be broken down into the following groups:

- settings creating the protection scope;
- settings determining the scan methods.

To edit IM Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
4. Make the required changes in the settings of the component selected.

IN THIS SECTION:

COMPONENT OPERATION ALGORITHM

Computer Protection includes a component that ensures the scan of messages transferred via IM (instant messaging) clients for dangerous objects, named *IM Anti-Virus*. It loads at the startup of operating system and runs in your computer's RAM, scanning all incoming and outgoing messages.

By default, protection of IM clients' traffic is carried out using the algorithm described below:

1. Each message received or sent by the user is intercepted by the component.
2. IM Anti-Virus scans the message for dangerous objects or URLs listed in databases of suspicious and/or phishing web addresses. If a threat is detected, message text will be substituted with a warning message for the user.
3. If no security threats are detected in the message, it becomes operable for the user.

Files transferred via IM clients are scanned by the File Anti-Virus component (see section "Computer file system protection" on page 59) when they are attempted to save.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages subject to scan:

- **Incoming and outgoing messages**. IM Anti-Virus scans both incoming and outgoing messages by default.
- **Incoming messages only**. If you are sure that messages sent by you cannot contain dangerous objects, select this setting. IM Anti-Virus will scan only incoming messages.

By default, Computer Protection scans both incoming and outgoing messages of IM clients.

If you are sure that the messages sent by you cannot contain any dangerous objects, you may disable the scan of outgoing traffic.

To disable the scan of outgoing messages, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
4. In the **Protection scope** section, select the **Incoming messages only** option for the component selected.

SELECTING THE SCAN METHOD

Scan methods consist in scanning the URLs in IM clients' messages to know if they are included in the list of suspicious web addresses and / or in the list of phishing web addresses:

- **Check if URLs are listed in the base of suspicious web addresses**. IM Anti-Virus will scan the links inside the messages to identify if they are included in the black list.
- **Check if URLs are listed in the base of phishing web addresses**. Computer Protection databases include all the sites currently known to be used for phishing attacks. Kaspersky Lab supplements this list with addresses obtained from the Anti-Phishing Working Group, which is an international organization. Your local copy of this list is updated when you update Computer Protection databases.

To scan links in the messages using the database of suspicious web addresses, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
4. In the **Scan methods** section, check the **Check if URLs are listed in the base of suspicious web addresses** box for the component selected.

To scan links in the messages using the database of phishing web addresses, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
4. In the **Scan methods** section, check the **Check if URLs are listed in the base of phishing web addresses** box for the component selected.

USING HEURISTIC ANALYSIS

Essentially, the heuristic method analyzes the object's activities in the system. For this purpose, any script included in an IM client's message is executed in the protected environment. If this script's activity is typical of malicious objects, the object is likely to be classed as malicious or suspicious. By default, heuristic analysis is enabled.

Computer Protection will notify you when a malicious object is detected in a message.

Additionally you can set the detail level for scans: **Light**, **Medium**, or **Deep**. To do so, move the slider bar to the selected position.

To enable/disable the heuristic analysis, and to set the detail level for the scan, please do the following:

1. Open the mainapplication window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **IM Anti-Virus** component.
4. In the **Scan methods** section, check / uncheck the **Heuristic analysis** box and set the scan detail level below for the component selected.

APPLICATION CONTROL

Based on the system security factor, all applications can be divided into three groups:

- *Safe*. This group includes applications developed by well-known vendors and provided with digital signatures. You may allow such applications to perform any actions in the system.
- *Dangerous*. This group includes currently known threats. Activity of applications included in this group must be blocked.
- *Unknown*. This group may include applications developed by unknown developers which are not provided with a digital signature. Such applications may or may not harm the system. You can make a firm decision if it is safe to use applications in this group only after you run them and analyze their behavior. Before you decide whether an unknown application is safe or unsafe, it would be reasonable to restrict its access to the system resources.

The Application Control component logs the actions performed by applications in the system, and manages the applications' activities, based on which group (see section "Application groups" on page 88) they belong to. A set of rules is defined for each group of applications (see section "Application Control rules" on page 90). These rules manage applications' access to various resources, such as:

- files and folders;
- registry keys;
- network addresses;
- execution environment.

When an application accesses a resource, the component checks if the application has the required access rights, and performs the action determined by the rule.

To modify the Application Control settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. Make the required changes in the settings for the component you have selected.

Also:

1. Open the main application window and selectthe **Application Control** section.
2. In the right part of the window, click the **Application activity** link.
3. In the **Application Activity Control** window that will open, make the required changes.

IN THIS SECTION:

COMPONENT OPERATION ALGORITHM

At the first startup of an application, Application Control analyzes it using the following algorithm:

1. Scans the application for viruses.

2. Verifies the application's digital signature. If the digital signature is confirmed, the application will be included in the **Trusted** group. If the application has no digital signature (or if the digital signature is corrupted, or included in the black list), the component will proceed to the next step.

3. Searches for a record of the application being started in the internal base of known applications included with Computer Protection installation package. If a record for the application being started is found in the base, it will be included in the corresponding group. If no record for the application being started is found in the base, the component will proceed to the next step.

4. Sends information about the application's executable file to the base of known applications stored at a Kaspersky Lab's server. If the base already contains a record related to the information sent, the application will be included in the corresponding group. If the base is inaccessible (for example, no Internet connection is active), the component will proceed to the next step.

5. Calculates the application's threat rating using the heuristic analysis. Applications with lower rating are placed into the **Low Restricted** group. If the application's rating is high, Computer Protection will notify you about it, and will offer you to select a group into which you should place this application.

When these scans are completed, a notification displays the final decision regarding the application. By default, the notification is disabled.

When the application is restarted, Application Control checks its integrity. If the application has not been changed, the component applies the existing rule to it. If the application has been changed, Application Control analyzes it using the algorithm described above.

SEE ALSO:

INHERITING RIGHTS

The important part of the Application Control component is the mechanism of the *access rights inheritance*. This mechanism prevents the use of trusted applications by a non-trusted application or an application with restricted rights in order to perform actions requiring certain privileges.

When an application attempts to obtain access to a monitored resource, Application Control analyzes the rights of all parent processes of this application, and compares them to the rights required to access this resource. At that, the *minimum priority rule* is observed: when comparing the access rights of the application to those of the parent process, the access rights with a minimum priority will be applied to the application's activity.

Access right priority:

1. **Allow**. Access right data have the highest priority.

2. **Prompt user**.

3. **Block**. Access right data have the lowest priority.

Example:

A Trojan attempts to use *regedit.exe* to edit the Microsoft Windows registry. The rule for the Trojan program sets the **Block** action as the reaction to an attempt to access the registry, while the rule for *regedit.exe* sets the **Allow** action.

As a result, activities of *regedit.exe* run by the Trojan will be blocked since the rights of *regedit.exe* will be inherited from the parent process. This event will trigger the minimum priority rule, and the action will be blocked despite the fact that the *regedit.exe* program has the rights required to allow it.

If the application's activities are blocked due to insufficient rights of a parent process, you can edit the rules (see section "Editing an application rule" on page 92).

You should modify the rights of a parent process only if you are absolutely certain that the process' activities do not threaten the system's security.

SEE ALSO:

THREAT RATING

Application Control determines the threat rating for every application running on your computer, using the heuristic analysis. The *threat rating* is the indicator of how dangerous the application is for the system; it is calculated based on two types of criteria:

- static (these criteria include information about the application's executable file: size, creation date, etc.);
- dynamic, which are used while simulating the application's operation in a virtual environment (analysis of the application's calls to system functions). Analyzing these criteria allows detecting a behavior typical of malware.

Based on rating values, Application Control divides applications into groups (see section "Application groups" on page 88). The lower the threat rating is, the more actions the application will be allowed to perform in the system.

APPLICATION GROUPS

All user's applications on the computer are divided by Application Control into groups, based on the level of danger for the system which in turn affects the applications' rights to access the system's resources.

There are four pre-set groups of applications:

- **Trusted**. Applications with a digital signature by trusted vendors, or applications which are recorded in the base of trusted applications. These applications have no restrictions applied on actions performed in the system. Those applications' activity is monitored by Proactive Defense and File Anti-Virus.
- **Low Restricted**. Applications that do not have a digital signature from a trusted vendor, and which are not listed in the base of trusted applications. However, these applications have received a low value of the threat rating (on page 88). They are allowed to perform some operations, such as access to other processes, system control, hidden network access. The user's permission is required for most operations.
- **High Restricted**. Applications without a digital signature and which are not listed in the base of trusted applications. These applications have a high value of the threat rating. The applications of this group require the user's permission for most actions which affect the system: some actions are not allowed for such applications.

- **Untrusted**. Applications without a digital signature and which are not listed in the base of trusted applications. These applications have received a very high value of the threat rating. Application Control blocks any actions performed by such applications.

The applications classed by Application Control in a certain group are assigned the corresponding status, and inherit the rights of access to the resources from the group rule (see section "Application Control rules" on page 90).

Kaspersky Lab advises you not to move applications from one group to another. Instead, if required, modify the application's rights to access specific system resources (see section "Editing an application rule" on page 92).

APPLICATION RUN SEQUENCE

Application startup may be initiated either by the user or by another application running.

If the startup is initiated by another application, it results in creating a startup procedure including parent and child programs. Startup procedures can be saved.

When saving a startup procedure, each program included in it remain in its group.

SEE ALSO:

Inheriting rights 87

CREATING A PROTECTION SCOPE

Application Control manages rights of user applications to perform actions with the following resource categories:

Operating system. This category includes:

- registry keys containing startup settings;
- registry keys containing internet use settings;
- registry keys affecting system security;
- registry keys containing system service settings;
- system files and folders;
- startup folders.

Kaspersky Lab has created a list of operating system's settings and resources which should always be protected by Computer Protection. This list cannot be edited. However, you can renounce the monitoring of any operating system object in the category you have selected, as well as add to the list.

Identity data. This category includes:

- user's files (My Documents folder, cookie files, information about the user's activity);
- registry files, folders and keys which contain the settings and important data of the most frequently used applications: Internet browsers, file managers, mail clients, IM clients, and electronic wallets.

Kaspersky Lab has created a list of resource categories which should always be protected by Computer Protection. This list cannot be edited. However, you can renounce the monitoring of any resource category, as well as add to the list.

To add to the list of identity data items to be protected, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Personal data** tab, in the **Category** dropdown list, select the required category of personal data objects, and click the **Add** link (or click the **Add category** link if you wish to add a new category of resources to be protected, and enter its name in the window that will open).
6. In the **User resource** window that will open, click the **Browse** button and specify required data, depending on the resource being added:

   - **File or folder**. In the **Select file or folder** window that will open, specify a file or a folder.
   - **Registry key**. In the **Please specify a registry object** window that will open, specify the registry key being protected.
   - **Network service**. In the **Network service** window that will open, specify the settings of monitored network connection (see section "Configuring network service settings" on page 105).
   - **IP addresses**. Specify the protected range of addresses in the **Network addresses** window that will open.

   After the resource has been added to the protection scope, you can edit or delete the resource using the corresponding links in the bottom part of the tab. To exclude the resource from the protection scope, uncheck the box ☑ next to it.

To add to the list of operating system's settings and resources to be protected, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Operating system** tab, in the **Category** dropdown list, select the required category of operating system objects, and click the **Add** link.
6. In the **User resource** window that will open, click the **Browse** button and specify required data, depending on the resource being added:

   - **File or folder**. In the **Select file or folder** window that will open, specify a file or a folder.
   - **Registry key**. In the **Please specify a registry object** window that will open, specify the registry key being protected.

   After the resource has been added to the protection scope, you can edit or delete the resource using the corresponding links in the bottom part of the tab. To exclude the resource from the protection scope, uncheck the box ☑ next to it.

APPLICATION CONTROL RULES

Rule is a set of reactions of Application Control to the application's actions on the resources being monitored (see section "Creating a protection scope" on page 89).

Possible component's reactions include the following:

- **Inherit**. For an application's activity, Application Control will apply the rule set for the group the application belongs to. This is the default setting for the reaction.
- **Allow**. Application Control allows an application to perform an action.
- **Deny**. Application Control does not allow an application to perform an action.
- **Prompt for action**. Application Control informs the user that an application is attempting to perform an action, and prompts the user for further actions.
- **Log events**. Information about an application's activity and Application Control's reaction will be logged in a report. Adding the information to a report can be used together with any other component's action.

By default, an application inherits the access rights from the group it belongs to. You can edit an application rule. In this case, the application rule's settings will have a higher priority than those inherited from the group the application belongs to.

SEE ALSO:

PLACING APPLICATIONS INTO GROUPS

Applications included by the Application Control component in the **Trusted** group (see section "Application groups" on page 88) do not impose any threat to the system.

You can use the option of specifying the range of trusted applications, activities of which will not be scanned by Application Control. Trusted applications may include those with a digital signature or those listed in Kaspersky Security Network's database.

For other applications, which do not fit into the trusted group, you can use heuristic analysis to determine a group, or specify a particular group into which the application will be added automatically.

For Application Control to view applications with a digital signature and / or contained in the Kaspersky Security Network database as trusted, and not to notify of their activity, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. In the **Trusted applications** section, check the ☑ **Applications with digital signature** box and / or the ☑ **Applications from Kaspersky Security Network database** box for the component selected.

- *If you want Application Control to use heuristic analysis for allocating untrusted applications to groups:*

  1. Open the main application window and click the **My Computer Protection** button.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, in the **Protection** section, select the **Application Control** component.
  4. Select the **Use heuristic analysis to define status** option in the **Trusted applications** section. When the status is assigned, the application will be attributed to the corresponding group.

- *If you want Application Control to assign the specified status automatically when allocating untrusted applications to groups:*

  1. Open the main application window and click the **My Computer Protection** button.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, in the **Protection** section, select the **Application Control** component.
  4. Select the **Assign the following status automatically** option in the **Trusted applications** section. Applications will be distributed to corresponding groups.

CHANGING THE TIME USED TO DETERMINE THE APPLICATION STATUS

If heuristic analysis is used to determine the application status, Application Control analyzes the program for 30 seconds by default. If threat rating has not been calculated during this time, the application receives a *Low Restricted* status and is placed to the corresponding group.

Threat rating calculation continues in the background. After the application has been studied with the help of heuristic analyzer, it receives the status according to its threat rating and is placed to the corresponding group.

You can change the time, allocated for applications analysis. If you are sure that all applications started on your computer do not impose any threat to security, you can decrease the time spent for analysis. If, on the contrary, you are installing the software and are not sure that it is safe, you are advised to increase the time for analysis.

- *To change the amount of time allocated to checking the unknown applications:*

  1. Open the main application window and click the **My Computer Protection**.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, in the **Protection** section, select the **Application Control** component.
  4. For selected component set the value for **Maximum time to define the application status** parameter in the **Additional** section.

EDITING AN APPLICATION RULE

When an application is started for the first time, Application Control determines its status and includes it in a certain group. After that, the component logs the actions performed by this application in the system, and manages its activity based on which group (see section "Application groups" on page 88) it belongs to. When an application accesses a resource, the component checks if the application has the required access rights, and performs the action determined by the rule. You can edit the rule that was created for the application when determining its status and including the application in the corresponding group.

- *To change an application rule, please do the following:*

  1. Open the main application window and click the **My Computer Protection**.
  2. In the window that will open, select the **Application Control** section.

3. In the window that will open, in the **Application Control** block, click the **Application activity** link.
4. In the **Application Activity Control** window that will open, in the **Category** dropdown list, select the required category.
5. In the **Status** column, left-click the link with the application's status for the required application.
6. In the menu that will open, select the **Custom settings** item.
7. In the window that will open, on the **Rules** tab, edit the access rules for the required resource category.

EDITING A RULE FOR AN APPLICATION GROUP

When an application is started for the first time, Application Control determines its status and includes it in a certain group. After that, the component logs the actions performed by this application in the system, and manages its activity based on which group (see section "Application groups" on page 88) it belongs to. You can edit the rule for the group, if necessary.

To change a rule for the group, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. In the **Rules for application statuses** block, click the **Configure rules** button for the component selected.
5. In the **Activity Control settings** window that will open, select the required group.
6. In the window that will open, on the **Rules** tab, edit the access rules for the required resource category.

CREATING A NETWORK RULE FOR APPLICATION

By default, after the first startup of the application, Application Control includes it in one of the preset groups. A group rule regulates an application's access to a network with a specified status. If you need to process the application's access to certain network services in a special way, you can create a network rule.

To create a rule controlling the application's network activity, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, select the **Application Control** section.
3. In the window that will open, in the **Application Control** block, click the **Application activity** link.
4. In the **Application Activity Control** window that will open, in the **Category** dropdown list, select the required category.
5. In the **Status** column, left-click the link with the application's status for the required application.
6. In the menu that will open, select the **Custom settings** item.
7. In the window that will open, on the **Rules** tab, select the **Network rules** category from the dropdown list, and click the **Add** link.
8. In the **Network rule** window that will open, configure the packet rule.
9. Assign the priority for created rule.

CONFIGURING EXCLUSIONS

When you create a default application rule, Computer Protection will monitor any of the user application's actions, including: access to files and folders, access to the execution environment, and network access. You can exclude certain actions of a user application from the scan.

In order to exclude applications' actions from the scan:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, select the **Application Control** section.
3. In the window that will open, in the **Application Control** block, click the **Application activity** link.
4. In the **Application Activity Control** window that will open, in the **Category** dropdown list, select the required category.
5. In the **Status** column, left-click the link with the application's status for the required application.
6. In the menu that will open, select the **Custom settings** item.
7. In the window that will open, on the **Exclusions** tab, check the boxes that correspond to the actions you want to exclude. When excluding the application's network traffic scan, configure additional exclusion settings.

   All exclusions created in the rules for user applications are accessible in the application settings window in the **Threats and exclusions** section.

DELETING RULES FOR APPLICATIONS

You can use the option of deleting the rules for applications, that have not been started for some time.

To delete rules for applications, that have not been started for a specified time period:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. For selected component check the **Delete rules for applications remaining inactive for more than** box in the **Additional** section and specify the necessary number of days in the field to the right.

SAFE MODE OF APPLICATIONS EXECUTION

Safe mode of applications execution is not available on computers running Microsoft Windows XP x64.

To ensure maximum security of operating system objects and of users' personal data, Kaspersky Lab has implemented the option of running third-party applications in a protected virtual environment named *Safe Run*.

You are advised to avoid running the applications whose authenticity is not evident to you, when working in Safe Run mode. This allows to avoid modifications in operating system objects which may lead to an improper functioning.

Functionalities of some applications in Safe Run mode may be reduced when started on computers running under Microsoft Windows Vista x64 and Microsoft Windows 7 x64. If such applications are started, the corresponding message will be displayed on the screen if you have configured the notifications about the **Application functionality is limited in safe mode** event.

Running Internet browsers in a safe environment ensures security when viewing web resources, including the protection against malware penetrating the computer and the protection of user data against any unauthorized attempts of changing and deleting, as well as the possibility of deleting all objects accumulated during the Internet session: temporary files, cookies, history of web pages browsed, etc. Microsoft Internet Explorer is included in the list of applications running in safe mode, by default.

Running an application in safe mode is performed depending on the mode selected. The option of creating shortcuts is provided for a quick start of applications in safe mode.

For the files saved or modified in safe mode to be available when working in standard mode, you should use the Safe Run Shared Folder created exclusively for those files and available both in safe mode and in standard mode. When clearing safe mode data (see page 98), the files stored in this folder will not be deleted.

You are advised to use Microsoft Windows standard mode to install the applications with which you wish to work in safe mode in the future.

IN THIS SECTION:

RUNNING AN APPLICATION IN SAFE MODE

If the **Always run in safe mode** option is not enabled for the application, it can be run in safe mode using one of the following ways:

- from the Microsoft Windows context menu;

- from the main window of My Computer Protection (see section "My Computer Protection" on page 53);
- using an existing shortcut (see section "Creating a shortcut for program execution" on page 96).

If the **Always run in safe mode** option is selected for the application, it will be launched in safe mode regardless of the run mode.

Applications running in safe mode, are highlighted with a green frame around the application window, and highlighted with green color in the list of applications monitored by Application Control (see section "Application Control" on page 86).

To run an application in safe mode using a shortcut, please do the following:

1. Open the folder in which a shortcut was created.
2. Run the application by double-clicking its shortcut.

To run an application in safe mode from the main window of My Computer Protection, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, select the **Application Control** section.
3. In the bottom part of the window, select the icon of the required application.
4. Double-click the icon to run the application, or open the context menu and select the **Run** item.

To run an application in safe mode from the Microsoft Windows context menu, please do the following:

1. Right-click thename of the object selected: of the application shortcut or executable file.
2. In the menu that will open, select the **Safe Run** item.

CREATING A SHORTCUT FOR PROGRAM EXECUTION

To run applications quickly in safe mode, Computer Protection provides the possibility of creating shortcuts. This allows running the required application in safe mode, without opening the main application window or the Microsoft Windows context menu.

To create a shortcut to run an application in safe mode, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, select the **Application Control** section.
3. In the bottom part of the window, in the **Safe Run applications** field, select the icon of the required application.
4. By right-clicking, open the context menu and use the **Create shortcut** item.
5. Specify the path for saving a shortcut and its name in the window that will open. By default, a shortcut will be created in the *My Computer* folder of the current user, and it will be assigned the name corresponding to the application's process.

CREATING THE LIST OF APPLICATIONS RUNNING IN SAFE MODE

You can create a list of applications running in safe mode in the main application window. The list is displayed in the **My Security Zone** section.

If you add to the list an application that allows working with several copies of it at the same time (such as Windows Internet Explorer), each new copy of it runs in safe mode after the application is added to the list. If you add to the list an application that allows using only one copy of it, that application must be restarted after it is added to the list.

To add an application in the list of applications running in safe mode, please do the following:

1. Open themain application window and click the **My Computer Protection** button.
2. In the window that will open, select the **Application Control** section.
3. In the bottom part of the window, in the **Safe Run applications** field, click the **Add** link.
4. In the menu that will open, select the necessary application. Once you select the **Browse** item, a window will open in which you should specify the path to an executable file. Once you select the **Applications** item, the list of applications currently running will open. After this, the application icon will be added in the field.

   To delete an application from the list of applications running in safe mode, select it in the list and click the **Delete** link.

SELECTING THE MODE: RUNNING AN APPLICATION

By default, all the applications installed on the computer can run both in standard mode and in safe mode. When adding an application in the list of applications running in safe mode, you can enable the **Always run in safe mode** option for it. This means that the application will be run in safe mode regardless of the run mode, whether using Microsoft Windows standard tools, or Computer Protection tools.

You are not advised to enable the **Always run in safe mode** option for system applications and utilities, since this can lead to an improper functioning of the operating system.

To run an application in safe mode only, regardless of the run mode, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, select the **Application Control** section.
3. In the bottom part of the window, select the icon of the required application.
4. By right-clicking, open the context menu.
5. Select the **Always run in safe mode** item. The ✓ box will be displayed next to the menu item.

   To allow the application to run in standard mode, select this item again.

SELECTING THE MODE: CLEARING SAFE MODE DATA

If an application runs in safe mode, all modifications performed by the application are performed within the scope of safe mode only. By default, at the next application startup, all changes made and files saved will be available during the safe mode session.

If you do not need the safe mode data any more, you can clear it (see page 98).

If you do not want the changes you have made to be available for an application at the next run in safe mode, you can enable the **Clear Safe Run data on exit** mode for it. This means that the changes you have made during the session, will be lost. Applications running in the specified mode, are marked with the  icon.

To clear Safe Run data every time the application closes, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, select the **Application Control** section.
3. In the bottom part of the window, select the icon of the required application.
4. By right-clicking, open the context menu.
5. Select the **Clear Safe Run data on exit** item. The box will be displayed next to the menu item and the sign will appear on the application icon in the list of applications running in safe mode.

   To disable clearing data saved during an application's session in safe mode, select this item again.

USING A SHARED FOLDER

When working in safe mode, all changes required due to the application's operation, are only made in safe mode, so they do not affect the standard mode. Thus, files saved in safe mode cannot be transferred to the standard mode.

For the files saved or modified in safe mode to be available in standard mode, *Safe Run Shared Folder* can be used, provided by Computer Protection. All files saved in this folder when working in safe mode, will be available in standard mode.

Shared folder is a folder on the hard drive created when you install Computer Protection.

The shared folder is created in the *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* folder during application installation, and its location cannot be changed.

The shared folder is indicated with the icon in the Microsoft Windows Explorer. You can also go to the folder from the Computer Protection's main window.

To open the shared folder from the Computer Protection's main window, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, select the **Application Control** section.
3. Click the **Shared Folder** link. The folder will open in a standard window of Microsoft Windows.

CLEARING THE SAFE MODE DATA

If you need to delete data saved in safe mode, or if you need to restore the current settings for all applications running in Microsoft Windows standard mode, you can clear safe mode data.

Before clearing the data, saved in the safe mode, you should make sure that all information you may need for further work has been saved in the shared folder. Otherwise, the data will be deleted without any possibility to restore them.

To clear safe mode data, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, select the **Application Control** section.
3. In the bottom part of the window, in the **Safe Run applications** field, click the **Clear** link.

4. In the window that will open, confirm data clearing by using the **OK** button, or click the **Cancel** button to cancel clearing.

FIREWALL

Computer Protection contains a special component, *Firewall*, to ensure your security on local networks and the Internet. It filters all network activities using rules of two types: *rules for applications* and *packet rules*.

Firewall analyzes settings of the networks to which you are connecting the computer. If the application runs in interactive mode (see section "Using interactive protection mode" on page 156), Firewall will request that you specify the status of the connected network, when first connected. If the interactive mode is off, the Firewall determines the status based on the network type, ranges of addresses and other specifications. Depending on the network status Firewall applies various rules to filtering network activities.

To modify Firewall's settings:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** and **Networks** tabs modify the settings of **Firewall** operation.

IN THIS SECTION:

CHANGING THE NETWORK STATUS

All network connections on your computer are monitored by Firewall. Firewall assigns a specific status to each connection and applies various rules for filtering of network activity depending on that status.

Once you get connected to a new network, Firewall will display a notification (see page 262) on the screen. To select a method for network activity filtering, you should specify the *status* for the detected network. You can select one of the following statuses:

- **Public network (Internet)**. We recommend that you select this status for networks not protected by any anti-virus applications, firewalls or filters (for example, for Internet cafe filters). Users of such networks are not allowed access to files and printers located on or connected to your computer. Even if you have created a shared folder, the information in it will not be available to users from networks with this status. If you allowed remote access to the desktop, users of this network will not be able to obtain it. Filtering of the network activity for each application is performed according to the rules for this application. By default, this status is assigned to Internet.
- **Local network**. We recommend that you assign this status to networks to which users you wish to grant access to files and printers on your computer (for example, for your internal corporate network or home network).

- **Trusted network**. This status is only recommended for areas that you consider absolutely safe within which your computer will not be subjected to attacks or unauthorized attempts to gain access to your data. If you select this status, all network activity is allowed within this network.

Types of network activities allowed for networks with a certain status depend on the settings of the default packet rules. You change these rules.

The network status defines the set of rules being used for filtering the network activities for the particular network.

To change the network connection status:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Networks** tab, select an active network connection and click the **Edit** link.
6. In the window that will open, on the **Properties** tab, select the required status from the dropdown list.

EXTENDING THE RANGE OF NETWORK ADDRESSES

Each network matches one or more ranges of IP address. If you connect to a network, access to subnetwork of which is performed via a router, you can manually add subnetworks accessible through it.

Example: you are connecting to the network in an office of your company and wish to use the same filtering rules for the office where you are connected directly and for the offices accessible over the network.

Obtain network address ranges for those offices from the network administrator and add them.

To extend the range of network addresses:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Networks** tab, select an active network connection and click the **Edit** link.
6. In the window that will open, on the **Properties** tab, in the **Additional subnetworks** block, click the **Add** link.
7. In the IP address window that will open, specify an **IP address** or an address mask.

SELECTING THE MODE OF NOTIFICATION ABOUT NETWORK CHANGES

Network connection settings can be changed during the work. You can receive notifications about the following changes:

- Connection to a network.
- In case of changes in the MAC address correspondence to the IP address. This notification will open once the IP address of one of the network computer will change.
- If a new MAC address appears. This notification opens once a new computer is added to the network.

In order to enable notification about changes of the network connection settings:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Networks** tab, select an active network connection and click the **Edit** link.
6. In the window that will open, on the **Additional** tab, check the boxes for the events about which you want to receive notifications.

ADVANCED FIREWALL SETTINGS

Advanced Firewall settings are as follows:

- Permission to use active FTP mode. Active mode suggests that to ensure connection between the server on the client computer a port to which the server will connect will be opened on the client computer (unlike the passive mode when the client connects to the server). The mode allows to control which exactly port will be opened. The mechanism works even if a blocking rule was created. By default, active FTP mode is allowed.
- Block connections if prompting for action is not available (application interface is not loaded). This setting allows to avoid disruption of the Firewall operation when the interface of Computer Protection is not loaded. This is the default action.
- Firewall functioning until complete system stop. This setting allows to avoid disruption of the Firewall operation until the system is completely stopped. This is the default action.

To modify advanced settings of the Firewall, perform the following steps:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** tab, click the **Additional** button.
6. In the **Additional** window that will open, make sure that the respective boxes are checked.

FIREWALL RULES

A Firewall *rule* is an action performed by Firewall once it detects a connection attempt with certain settings: direction and protocol of the data transfer, range of addresses and ports to which the connection is performed.

Firewall works based on rules of two types:

- *Packet rules* (see section "Creating a packet rule" on page 103) are used for imposing restrictions on data packets and streams irrespective of the applications.
- *Rules for applications* (see section "Creating a rule for the application" on page 103) are used for imposing restrictions on the network activity of a certain application. Such rules allow fine-tuning the filtering, for example, when a certain type of data stream is banned for some applications but is allowed for other ones.

Packet rules have a higher priority compared to the application rules. If both packet rules and application rules are applied to the same type of network activity, this network activity will be processed using the packet rules.

SEE ALSO:

CREATING A PACKET RULE

Typically, packet rules restrict inbound network activity on specified TCP and UDP ports and filter ICMP messages.

A packet rule consists of a set of conditions and operations over packets and data streams performed when these conditions are met.

When creating packet rules, remember that they have the priority over application rules.

While creating the rule's conditions you can specify the network service and the network address. You can use an IP address as the network address or specify the network status. In the latter case the addresses will be copied from all networks that are connected and have the specified status at this moment.

To create packet rule:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** tab, select the **Packet rules** block and click the **Add** link.
6. In the **Network rule** window that will open, specify the rule settings.
7. Assign the priority for created rule.

After you have created the rule, you can modify its settings or delete it using links in the bottom part of the tab. To disable the rule uncheck the ☑ box next to the rule's name.

CREATING A RULE FOR APPLICATION

Firewall analyzes the activity of each application running on your computer. Depending on the threat rating, every application is included to one of the following groups:

- **Trusted**. Applications of that group are allowed to perform any network activity irrespectively of the network status.

- **Low Restricted**. Applications of that group are allowed to perform any network activity in non-interactive mode. If you are using the interactive mode, a notification will be displayed on the screen using which you can allow or block a connection, or create an application rule using the Wizard (see section "Rule Creation Wizard" on page 104).

- **High Restricted**. Applications of that group are not allowed to perform network activity in non-interactive mode. If you are using the interactive mode, a notification will be displayed on the screen using which you can allow or block a connection, or create an application rule using the Wizard (see section "Rule Creation Wizard" on page 104).

- **Untrusted**. Any network activity is prohibited for the applications of that group.

You can modify rules for a whole group or for a certain application in group, and also create additional rules for more accurate filtering of network activity.

Custom rules for individual applications have a higher priority than the rules inherited from a group.

After the application activity analysis, Firewall creates rules regulating application's access to networks with specific status. You can create additional rules for more flexible management of Computer Protection's network activity.

To create an application rule, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** tab, select a group of rules for the application and click the **Add** link.
6. In the **Network rule** window that will open, specify the rule settings.
7. Assign the priority for created rule.

After you have created the rule, you can modify its settings or delete it using links in the bottom part of the tab. To disable the rule uncheck the ☑ box next to the rule's name.

RULE CREATION WIZARD

If a rule gets triggered and it is configured to **Prompt for action** (the action is set by default for the applications included in the **Low Restricted** or **High Restricted** groups (see section "Application groups" on page 88)), a corresponding notification (see page 261) is displayed on the screen. You can select possible further actions in the notification window:

- **Allow**.

- **Deny**.

- **Create a rule**. When this option is selected, *Rule Creation Wizard* is started, which will help you to create a rule, controlling network activity of the application.

The action in a triggered rule can be changed to **Allow** or **Deny**; to do that you should check the ☑ **Always apply for this application** box.

The wizard consists of several dialogs (steps) navigated using the **Back** button and the **Next** link; it completes its work after clicking the **Finish** link. To stop the wizard at any stage, use the **Cancel** button.

SELECTING ACTIONS TO BE PERFORMED BY THE RULE

When a rule is applied, the Firewall performs with a packet or data stream one of the following operations:

- **Allow**.
- **Block**.
- **Process according to application rules**. In this case processing of such data packet or stream by the packet rule will be stopped. Application rules are applied to connections.

If you wish to log information about a connection attempt and the Firewall actions, enable the **Log events** mode.

In order to change an action performed by Firewall:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** tab, click the **Add** link.
6. In the **Network rule** window that will open, in the **Action** block, select an action.

CONFIGURING NETWORK SERVICE SETTINGS

Settings characterizing the activity of the network for which a rule is created are described by the *network service*. Network service has the following settings:

- *Name*. This text is displayed in the list of available network services which can be selected.
- *Direction*. Firewall monitors connections with the following directions:
  - **Inbound**. A rule is applied to data packets received by your computer. It is not applied in the application rules.
  - **Inbound (stream)**. The rule is applied to network connections opened by a remote computer.
  - **Inbound / Outbound**. The rule is applied both to the incoming and the outgoing data stream regardless of what computer, yours or a remote computer, initiated the network connection.
  - **Outbound**. A rule is applied to data packets transferred from your computer. It is not applied in the application rules.
  - **Outbound (stream)**. The rule is only applied to network connections opened by your computer.
- *Protocol*. Firewall monitors connections using TCP, UDP, ICMP, ICMPv6, IGMP and GRE protocols. If protocol ICMP or ICMPv6 was selected as the protocol, you can specify the type and the code of the ICMP packet.

Application rules control connections only via TCP and UDP protocols.

- *Remote and local ports*. For TCP and UDP protocols you can specify ports of your computer and the remote computer the connection between which will be monitored.

Computer Protection includes network services that describe most commonly used network connections. When creating Firewall rules, you can select one of the pre-installed network services or create a new network service.

In order to configure the settings of the network connection, processed by the rule:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** tab, click the **Add** link.
6. In the **Network rule** window that will open, in the **Network service** block, click the **Add** link.
7. In the **Network service** window that will open, specify the network connection settings.

SELECTING ADDRESSES RANGE

Firewall rules are applied to the following categories of network addresses:

- **Any address** – the rule will be applied to any IP address;
- **Subnetwork addresses with status** – the rule will be applied to IP addresses of all networks that are connected and have the specified status at the moment;
- **Addresses from group** – the rule will be applied to IP addresses included into the specified range.

In order to specify the IP address range to which the rule will be applied:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Firewall** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Filtering rules** tab, click the **Add** link.
6. In the **Network rule** window that will open, in the **Addresses** block, specify the range of addresses:
   a. if you preset **Subnetwork addresses with status** option, select the network status from the dropdown menu;
   b. select one of the existing groups of addresses if you specified the **Addresses from group** option. If you do not wish to use range of addresses from any group, create a new group. To do so, click the **Add** link in the bottom part of the block and specify the addresses included into the group in the **Network addresses** window that will open.

PROACTIVE DEFENSE

Computer Protection protects both from known threats, and from new threats, information about which is not contained in Computer Protection databases. This feature is ensured by a specially developed component named *Proactive Defense*.

The preventative technologies provided by Proactive Defense neutralize new threats before they harm your computer. In contrast with reactive technologies, which analyze code based on records in Computer Protection databases, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a program. If, as a result of activity analysis, the sequence of application's actions arouses any suspicion, Computer Protection blocks the activity of this application.

Activity analysis is performed for all applications, including those grouped as **Trusted** by the Application Control component (on page 86). For these applications you can disable notifications of Proactive Defense.

As opposed to the Application Control component, Proactive Defense reacts immediately to a defined sequence of an application's actions.

To edit Proactive Defense settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
4. Make the required changes in the settings for the component you have selected.

IN THIS SECTION:

USING THE LIST OF DANGEROUS ACTIVITY

Note that configuring the settings for activity control in Computer Protection under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 or Microsoft Windows 7 x64 differs from the same process under other operating systems.

Specifics of configuring application activity control under Microsoft Windows XP

Computer Protection monitors application activity on your computer. Proactive Defense reacts immediately to a defined sequence of application actions. For example, when actions such as a program copying itself to network resources, the startup folder or the system registry, and then sending copies of itself, are detected, it is highly likely that this program is a worm. Other dangerous sequences of operations include:

- actions, typical of Trojans;
- keyboard interception attempts;
- hidden driver installation;

- attempts to modify the operating system kernel;
- attempts to create hidden objects and processes with negative PID;
- HOSTS file modification attempts;
- attempts to implement in other processes;
- rootkits redirecting data input / output;
- attempts of sending DNS requests.

The list of dangerous activities is appended automatically when Computer Protection is updated, and it cannot be edited. However you can turn off monitoring for one dangerous activity or another.

To turn off monitoring for one dangerous activity or another:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
4. Click the **Settings** button for the component you have selected.
5. In the **Proactive Defense** window that will open, uncheck the box next to the name of the activity which you do not want to be monitored.

Specifics of configuring application activity control under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7, or Microsoft Windows 7 x64

If the computer is running under one of the above-mentioned operating systems, then control will not apply to each event; this is due to particular features of these operating systems. For example, control will not apply to the following event types: *sending data through trusted applications*, *suspicious system activities*.

CHANGING THE DANGEROUS ACTIVITY MONITORING RULE

The list of dangerous activities is appended automatically when Computer Protection is updated, and it cannot be edited. You can:

- turn off monitoring for one dangerous activity or another (see page 107);
- edit the rule that Proactive Defense uses when it detects dangerous activity;
- create an exclusion list (see page 167), by listing applications with activity that you do not consider dangerous.

To change the rule:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
4. Click the **Settings** button for the component you have selected.
5. In the **Proactive Defense** window that will open, in the **Events** block, select the required event for which you want to edit the rule.
6. Configure the settings for the selected event using the links in the rule description section:

- click the link with the preset action and select the required action in the **Select action** window that will open;
- click the link with the preset time period (not for any activity type) and specify the scan interval for hidden processes in the **Hidden processes detection** window that will open;
- click the On / Off link to indicate that the report on task execution should be created.

CREATING A GROUP OF TRUSTED APPLICATIONS

Applications included by the Application Control component in the **Trusted** group (see section "Application groups" on page 88) do not impose any threat to the system. However, their activities will also be monitored by Proactive Defense.

Use the option of specifying the range of trusted applications, activities of which will not be scanned by Proactive Defense. Trusted applications may include those with a digital signature or those listed in Kaspersky Security Network's database.

For Proactive Defense to view applications with a digital signature and / or contained in the Kaspersky Security Network database as trusted, and not to notify of their activity, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
4. In the **Trusted applications** section, check the **Applications with digital signature** box and / or the **Applications from Kaspersky Security Network database** box for the component selected.

SYSTEM ACCOUNTS CONTROL

User accounts control access to the system and identify the user and his/her work environment, which prevents other users from corrupting the operating system or data. System processes are processes launched by system user accounts.

If you want Computer Protection to monitor the activity of system processes in addition to user processes, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Proactive Defense** component.
4. In the **Additional** section, check the **Monitor system user accounts** box for the component selected.

NETWORK ATTACK BLOCKER

The *Network Attack Blocker* loads at the operating system startup, and tracks incoming network traffic for activities characteristic of network attacks. Once an attempt of attacking your computer is detected, Computer Protection blocks any network activity of the attacking computer towards your computer. By default, the blocking persists for one hour. A notification (see section "Notifications" on page 256) will appear on the screen informing of a network attack attempt perpetrated, with specific information about the computer which attacked you.

Descriptions of currently known network attacks (see section "Types of detected network attacks" on page 110) and methods to counteract them, are provided in the Computer Protection databases. The list of attacks which the Network Attack Blocker can detect is updated when the application's databases are updated.

IN THIS SECTION:

BLOCKING THE ATTACKING COMPUTERS

By default, Network Attack Blocker (on page 110) blocks the activity of an attacking computer for one hour.

To modify the time for which the attacking computer will be blocked:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Network Attack Blocker** component.
4. Check the **Add attacking computer to blocked list for** box for the component selected, and enter the blocking time.

To unblock the attacking computer:

1. Open the main application window and select the **My Protection** section.
2. In the right part of the window, in the **Online activity** section, click the **Network Monitor** link.
3. In the window that will open, on the **Blocked computers** tab, select the blocked computer and click the **Unblock** link.

TYPES OF DETECTED NETWORK ATTACKS

There are currently a multitude of various network attacks that utilize vulnerabilities in operating systems and other software, system-type or otherwise, installed on your computer.

To ensure the security of your computer, you must know what kinds of network attacks you might encounter. Known network attacks can be divided into three major groups:

1. *Port scan* – this threat type is not an attack itself but it usually precedes one since it is one of the common ways of obtaining information about a remote computer. The UDP/TCP ports used by the network tools on the computer targeted by an intruder are scanned to find out their status (closed or open).

   Port scans can tell a hacker what types of attacks will work on that system, and what types will not. In addition, the information obtained by the scan (a model of the system) will help the malefactor to know what operating

system the remote computer uses. This in turn further restricts the number of potential attacks, and, correspondingly, the time spent perpetrating them. It also aids a hacker in attempting to use vulnerabilities characteristic of the operating system.

2. *DoS attacks*, or Denial of Service attacks are the attacks, which cause an unstable performance of a system or its crash. Attacks of this type may affect the operability of information resources under attack (for example, blocking of Internet access).

   There are two basic types of DoS attacks:

   - sending the target computer specially created packets that the computer does not expect, which cause the system either to restart or to stop;
   - sending the target computer many packets within a timeframe that the computer cannot process, which cause system resources to be exhausted.

   The most flagrant examples for this group of attacks are the following types:

   - The *Ping of death* attack consists of sending an ICMP packet with a size greater than the maximum of 64 KB. This attack can crash some operating systems.
   - *Land attack* consists of sending a request to an open port on the target computer to establish a connection with itself. This sends the computer into a cycle, which intensifies the load on the processor and can lead to crashing of some operating systems.
   - The *ICMP Flood* attack consists of sending a large quantity of ICMP packets to your computer. The computer attempts to reply to each inbound packet, which slows the processor to a crawl.
   - The *SYN Flood* attack consists of sending a large quantity of queries to a remote computer to establish a fake connection. The system reserves certain resources for each of those connections, which completely drains your system resources, and the computer stops reacting to other connection attempts.

3. *Intrusion attacks*, which aim to take over your computer. This is the most dangerous type of attack, because if it is successful, the hacker takes total control of your system.

   Hackers use this attack to obtain confidential information from a remote computer (for example, credit card numbers, passwords), or to penetrate the system to use its computing resources for malicious purposes later (e.g., to use the invaded system in a zombie network, or as a platform for new attacks).

   This group is the largest by the number of attacks included. They may be divided into three groups depending on the operating system installed on the user's computer: Microsoft Windows attacks, Unix attacks, and the common group for network services available in both operating systems.

   The following types of attacks are the most wide-spread among those using the network resources of operating systems:

   - *Buffer overflow attacks* is a type of software vulnerability caused by a lack (or deficiency) of control when working with data arrays. This is one of the oldest vulnerability types and the easiest for hackers to exploit.
   - *Format string attacks* is a type of software vulnerability that arises from insufficient control of input values for I/O functions such as *printf()*, *fprintf()*, *scanf()*, and others, from the C standard library. If a program has this vulnerability, the hacker able to send queries created with a special technique, can take total control of the system.

   Intrusion Detection System automatically analyzes and prevents attempts to exploit these vulnerabilities in the most common network services (FTP, POP3, IMAP) if they are running on the user's computer.

   Attacks aimed at computers with Microsoft Windows are based on the use of vulnerabilities of the software installed on a computer (such as Microsoft SQL Server, Microsoft Internet Explorer, Messenger, and system components available via the network – DCom, SMB, Wins, LSASS, IIS5).

   In addition, there are isolated incidents of intrusion attacks using various malicious scripts, includes scripts processed by Microsoft Internet Explorer and Helkern-type worms. The essence of this attack type consists of sending a special type of UDP packets to a remote computer that can execute malicious code.

ANTI-SPAM

Computer Protection includes *Anti-Spam*, a component that allows detection of unwanted messages (spam) and their processing in accordance with the rules in your email client, which saves time when working with email.

Anti-Spam uses a self-training algorithm (see section "Component operation algorithm" on page 114) that allows the component to tell spam from useful mail better as time passes. The source of data for the algorithm is the contents of the message. To enable efficient recognition of spam and useful mail by Anti-Spam, the component needs training (see section "Training Anti-Spam" on page 115).

We strongly recommend that you review the Anti-Spam algorithm in detail!

Anti-Spam is built into the following mail clients as a plug-in:

- Microsoft Office Outlook (see section "Configuring spam processing in Microsoft Office Outlook" on page 127);
- Microsoft Outlook Express (Windows Mail) (see section "Configuring spam processing in Microsoft Outlook Express (Windows Mail)" on page 129);
- The Bat! (see section "Configuring spam processing in The Bat!" on page 129);
- Thunderbird (see section "Configuring spam processing in Thunderbird" on page 130).

You can use the lists of allowed (see page 122) and blocked (see page 120) senders to specify for Anti-Spam the addresses from which messages will be recognized as useful mail or spam. Moreover, Anti-Spam can check a message for the presence of phrases from the allowed (see page 123) and blocked (see page 121) lists, and also from the list of obscene (see page 122) expressions.

Anti-Spam allows you to view mail at the server (see section "Filtering email messages at the server. Mail Dispatcher" on page 126) and delete unwanted messages without downloading them to your computer.

To edit Anti-Spam settings:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. Make the required changes in the component settings.

IN THIS SECTION:

COMPONENT OPERATION ALGORITHM

Anti-Spam work consists of two stages:

1. Application of strict filtering criteria to a message. These criteria allow a quick determination as to whether the message is spam or not. Anti-Spam assigns to the message *spam* or *not spam* status, the scan will be stopped and the message will be transferred to the mail client for processing (see Steps 1 through 5 below).

2. Inspection of messages, which have passed strict selection criteria during previous steps. Such messages cannot be unambiguously considered spam. Therefore Anti-Spam has to calculate for them the *probability* of being spam.

Anti-Spam algorithm consists of the following steps:

1. Address of message sender is checked for the presence in the lists of allowed or blocked senders.

   - If a sender's address is in the allowed list, the message receives the *Not Spam* status.

   - If a sender's address is in the black list, the message receives the *Spam* status.

2. If a message was sent using Microsoft Exchange Server and scanning of such messages is disabled (see page 127), the message will be assigned the *not spam* status.

3. Message analysis is performed to check if it contains strings from the list of allowed phrases (see page 123). If at least one line from this list has been found, the message will be assigned the *not spam* status. This step is skipped by default.

4. Message analysis is performed to check if it contains strings from the list of blocked phrases (see page 121). Detection of words from this list in the message increases the chances of the messages being spam. If calculated probability exceeds the specified value (see page 124), a message receives the *Spam* or *Probable spam* status. Message analysis is performed to check if it contains strings from the list of obscene phrases (see page 122). This step is skipped by default.

5. If message text contains an address included into the database of phishing or suspicious web addresses (see page 119), the message receives the *Spam* status.

6. Message analysis using heuristic rules is performed. If the analysis reveals in a message signs typical of spam, the probability of its being spam increases.

7. The application analyzes the email message using the GSG technology. While doing it, Anti-Spam analyzes images attached to the email message. If analysis reveals in the images signs typical of spam, the probability of the message being spam increases.

8. The application analyzes the *.rtf* format documents attached to the message. It scans attached documents checking them for the presence of spam signs. After the analysis is complete, Anti-Spam calculates how much the probability of the message being spam increased. By default, the technology is disabled.

9. It checks for the presence of the additional features (see page 125) typical of spam. Each detected feature increases the probability that the message being scanned is in fact spam.

10. If Anti-Spam was trained, the message will be scanned using iBayes technology. Self-training iBayes algorithm calculates the probability of message being spam based on the frequency of phrases typical of spam found in message text.

Message analysis determines the probability of its being spam. Spam authors keep improving the methods they use to disguise spam; therefore, calculated probability most often does not reach the specified value (see section "Determining spam and potential spam ratings" on page 124). To ensure efficient filtering of the email message stream, Anti-Spam uses two parameters:

- *spam rating* – the probability value, which will cause the message to be considered *spam* when exceeded. If the probability is below this threshold value, the message is assigned the *potential spam* status;

- *potential spam rating* – the probability value, which will cause the message to be considered potential spam when exceeded. If the probability is less than this value, Anti-Spam will consider the message not spam.

Depending on the specified spam and potential spam ratings, messages will be assigned the *spam* or *potential spam* status. Based on the assigned status, messages will be also marked with the **[!! SPAM]** or **[!! Probable Spam]** label in the **Subject** field. Then they are processed according to the rules (see section "Actions to be performed on spam" on page 127) you have created for your mail client.

TRAINING ANTI-SPAM

One of the most powerful spam detection tools is the self-training iBayes algorithm. The algorithm decides, which status should be assigned to a message based on the phrases it contains. Before starting, sample strings of useful and spam mail should be submitted to the iBayes algorithm, i. e. it should be trained.

There are several approaches to training Anti-Spam:

- Using the Training Wizard (see section "Training using the Training Wizard" on page 116) (packet training). Training with the Training Wizard is preferable from the very onset of using Anti-Spam.

- Training Anti-Spam using outgoing messages (see section "Training Anti-Spam using outgoing messages" on page 117).

- Training directly while working with email (see section "Training using email client" on page 117), using special toolbar buttons or menu items.
- Training when working with Anti-Spam reports (see section "Training with reports" on page 118).

TRAINING USING THE TRAINING WIZARD

Training Wizard allows Anti-Spam training in batch mode. To do so, specify which folders of Microsoft Office Outlook or Microsoft Outlook Express accounts contain spam and useful mail.

Correct spam recognition requires training using at least 50 useful messages and 50 samples of unwanted mail. iBayes will not be operational until these steps are completed.

To save time the Training Wizard only trains on 50 emails in each selected folder.

This wizard consists of a series of windows (steps) navigated using the **Back** and **Next** buttons; to close the wizard, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. In the **Anti-Spam training** section, click the **Train** button for the component selected.

When performing training based on good email messages addresses of the message senders will be added to the list of allowed senders.

To disable addition of the sender's address to the list of allowed senders, perform the following steps:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it is from allowed sender** box and click the **Select** button.
6. In the **List of allowed senders** window that will open, uncheck the **Add allowed senders addresses when training Anti-Spam in the mail client** box.

SEE ALSO:

Training with reports 118

Training using email client 117

Training Anti-Spam using outgoing messages 117

TRAINING ANTI-SPAM USING OUTGOING MESSAGES

You can train Anti-Spam using a sample of 50 outgoing emails. The receivers' addresses will automatically be added to the list of allowed senders.

To train Anti-Spam on outgoing emails:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Additional** tab, in the **Outgoing messages** block, check the **Train using outgoing email messages** box.

To disable adding the sender's address to the list of allowed senders:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it is from allowed sender** box and click the **Select** button.
6. In the **List of allowed senders** window that will open, uncheck the **Add allowed senders addresses when training Anti-Spam in the mail client** box.

SEE ALSO:

Training using the Training Wizard 116

Training with reports 118

Training using email client 117

TRAINING USING EMAIL CLIENT

Training Anti-Spam while working directly with email messages involves using special interface elements of your mail client program.

Buttons used for training Anti-Spam appear in the interface of Microsoft Office Outlook and Microsoft Outlook Express (Windows Mail) mail clients only after you have installed Computer Protection.

To train Anti-Spam using the email client:

1. Start the email client.
2. Select a message using which you wish to train Anti-Spam.
3. Perform the following steps depending upon your email client:

- click the **Spam** or **Not Spam** button in the Microsoft Office Outlook toolbar;
- click the **Spam** or **Not Spam** button in the Microsoft Outlook Express toolbar (Windows Mail);
- use the special **Mark as Spam** and **Mark as Not Spam** items in the **Special** menu of The Bat! email client program;
- use the **Spam / Not Spam** button in the Mozilla Thunderbird toolbar.

After selection of an option from the list above Anti-Spam performs training using the selected message. If you select several messages, they will all be used for training.

If a message is marked as useful mail, the address of its sender will be added to the list of allowed senders.

To disable adding the sender's address to the list of allowed senders:

1. Open the mainapplication window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as not spam** block, check the ☑ **If it is from allowed sender** box and click the **Select** button.
6. In the **List of allowed senders** window that will open, uncheck the ☑ **Add allowed senders addresses when training Anti-Spam in the mail client** box.

In cases when you need to select several messages at the same time, or are certain that a folder contains messages of one and only group (spam or not spam), you can take a multi-faceted approach to component training using Training Wizard (see section "Training Anti-Spam" on page 115).

SEE ALSO:

TRAINING WITH REPORTS

Anti-Spam training can be performed using its reports as the source. The component's reports can help you assess the accuracy of the component's configuration, and if necessary, make certain corrections to Anti-Spam.

To mark a certain message as spam or not spam:

1. Open the main application window.
2. Click the **Report** link to switch to the reports window of Computer Protection.
3. In the window that will open, on the **Report** tab, click the **Detailed report** button.
4. For the **Anti-Spam** component select an email which you wish to use for additional training.
5. Open the shortcut menu for the message and select one of the following actions:

- **Mark as Spam**;
- **Mark as Not Spam**;
- **Add to the list of allowed senders**;
- **Add to the list of blocked senders**.

SEE ALSO:

Training Anti-Spam using outgoing messages 117

Training using the Training Wizard 116

Training using email client 117

CHANGING SECURITY LEVEL

To filter messages, the Anti-Spam component uses two factors:

- *Spam rating* – the probability value, which will cause the message to be considered spam when exceeded. If the probability is below this threshold value, the message is assigned the *potential spam* status.
- *Potential spam rating* – the probability value, which will cause the message to be considered potential spam when exceeded. If the probability is less than this value, Anti-Spam will consider the message not spam.

Kaspersky Lab specialists distinguish three security levels:

- **High**. This security level should be used if you receive spam frequently; for example, while using free mail services. When you select this level, the frequency of false positives rises: that is, useful mail is more often recognized as spam.
- **Recommended**. This security level should be used in most cases.
- **Low**. This security level should be used if you rarely receive spam, for example, if you are working in a protected corporate email environment. When this level is selected, spam and potential spam messages are less frequently recognized.

In order to change the selected Anti-Spam component security level:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Set the required security level for the component you have selected.

SELECTING THE SCAN METHOD

Scan methods consist in scanning the URLs in the messages of IM clients to know if they are included in the list of suspicious web addresses and / or the list of phishing web addresses.

Checking the links if they are included in the list of phishing addresses allows to avoid phishing attacks, which look like email messages from would-be financial institutions that contain links to their websites. The message text convinces the reader to click the link and enter confidential information in the window that follows, for example, a credit card number or a login and password for an Internet banking site where financial operations can be carried out.

A phishing attack can be disguised, for example, as a letter from your bank with a link to its official web site. By clicking the link, you go to an exact copy of the bank's website and can even see the real address in the browser, even though you are actually on a counterfeit site. From this point forward, all your actions on the site are tracked and can be used to steal your money.

To scan links in the messages using the database of suspicious addresses, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as spam** block, check the **If it contains URLs from the base of suspicious web addresses** box.

To scan links inside the email messages using the database of phishing addresses, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as spam** block, check the **If it contains URLs from the base of phishing web addresses** box.

CREATING THE LIST OF TRUSTED URLS

You can create a list of trusted addresses. Anti-Spam will check if the recipient's address is included into the list.

To create the list of trusted addresses:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, check the **If it is not addressed to me** box and click the **My addresses** button.
6. In the **My Email Addresses** window that will open, click the **Add** link.
7. Specify the required addresses or address masks in the **Email address mask** window that will open.

CREATING THE LIST OF BLOCKED SENDERS

The list of blocked senders contains the addresses of senders of messages which have been marked as spam. The list is filled manually.

The list can contain either addresses or address masks. When entering a mask, you can use the standard ***** and **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character. Examples of address masks:

- *ivanov@test.ru*. Messages from this address will always be classified as spam.
- **@test.ru.* Mail from any sender from the *test.ru* mail domain will always be considered spam; for example: *petrov@test.ru*, *sidorov@test.ru*.
- *ivanov@**. The sender with this name, regardless of the mail domain, always sends only spam; for example: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test**. Mail from any sender from a mail domain, starting with *test*, are considered spam; for example: *ivanov@test.ru*, *petrov@test.com*.
- *ivan.*@test.???*. Mail from a sender, whose name starts with *ivan.* and from mail domain beginning with *test* and ending in any three characters, is always spam, for example: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

In order to create a list of blocked senders and use it in your further work:

1. Open the main applicationwindow and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as spam** block, check the **If it is from blocked sender** box and click the **Select** button.
6. In the **List of blocked senders** window that will open, click the **Add** link.
7. In the **Email address mask** window that will open, enter the required address or mask.

CREATING THE LIST OF BLOCKED PHRASES

The list of blocked phrases is used to store key fragments of messages, which you consider to be spam. The list is filled manually.

You can also use masks for phrases. When entering a mask, you can use the ***** and **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character. Examples of phrases and phrase masks:

- *Hi, Ivan!.* An email message that contains this text only is a spam. The use of the lines similar to the following lines is not recommended.
- *Hi, Ivan!**. Message beginning with the *Hi, Ivan!* string is spam.
- *Hi, *! *.* Mail beginning with *Hi* and an exclamation mark in any part of the message is spam.
- ** Ivan? *.* Mail beginning with *Ivan* personal address followed by any character is spam.
- ** Ivan\? **. An email message containing the *Ivan?* phrase is spam.

If characters * and ? are included into a phrase, then they should be preceded by the \ character to prevent their misrecognition in Anti-Spam. Then two characters are used instead of one: * and \?.

To create the list of blocked phrases:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Exact methods** tab, in the **Consider message as spam** block, check the **If it contains blocked phrases** box and click the **Select** button.

6. In the **List of blocked phrases** window that will open, click the **Add** link.

7. In the **Blocked phrase** window that will open, enter a line or a mask.

CREATING THE LIST OF OBSCENE PHRASES

The list contains obscene phrases that indicate a spam message with high probability, if present.

Kaspersky Lab specialists have compiled the list of obscene phrases included in the distribution package of Computer Protection. You can edit this list.

You can also use masks for phrases. When entering a mask, you can use the ***** and **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character.

If characters * and ? are included into a phrase, then they should be preceded by the \ character to prevent their misrecognition in Anti-Spam. Then two characters are used instead of one: * and \?.

To edit the list of obscene phrases, perform the following steps:

1. Open the main applicationwindow and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Exact methods** tab, in the **Consider message as spam** block, check the **If it contains blocked phrases** box and click the **Select** button.

6. In the **List of blocked phrases** window that will open, check the **Consider as blocked obscene words** box and click the **obscene words** link.

7. Read the text in the **Agreement** window that will open and, if you accept the terms and conditions stated in the window, check the respective box and click the **OK** button.

8. In the **List of obscene words** window that will open, click the **Add** link.

9. In the **Blocked phrase** window that will open, enter a line or a mask.

CREATING THE LIST OF ALLOWED SENDERS

The list of allowed senders contains the addresses of message senders from whom, in your opinion, no spam is received. The list of addresses is filled automatically during Anti-Spam training. You can edit this list.

The list can contain either addresses or address masks. When entering a mask, you can use the standard ***** and **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character. Examples of address masks:

- *ivanov@test.ru.* Messages from this address will always be classified as good mail.
- **@test.ru.* Mail from any sender from the *test.ru* mail domain will always be considered good mail; for example: *petrov@test.ru*, *sidorov@test.ru*.

- *ivanov@*.* The sender with this name, regardless of the mail domain, always sends only good mail; for example: *ivanov@test.ru*, *ivanov@mail.ru*.
- **@test*.* Mail from any sender from a mail domain, starting with *test*, are considered not spam; for example: *ivanov@test.ru*, *petrov@test.com*.
- *ivan.*@test.???.* Mail from a sender, whose name starts with *ivan.* and from mail domain beginning with *test* and ending in any three characters, is always useful, for example: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

To create the list of allowed senders:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it is from allowed sender** box and click the **Select** button.
6. In the **List of allowed senders** window that will open, click the **Add** link.
7. In the **Email address mask** window that will open, enter the required address or mask.

CREATING THE LIST OF ALLOWED PHRASES

The list of allowed phrases is used to store key fragments of messages, which you have marked as useful mail. You can create such a list.

You can also use masks for phrases. When entering a mask, you can use the ***** and **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character. Examples of phrases and phrase masks:

- *Hi, Ivan!.* An email message that contains this text only is a good email. The use of the lines similar to the following lines is not recommended.
- *Hi, Ivan!**. Message beginning with the *Hi, Ivan!* string belongs to useful mail.
- *Hi, *! **. Mail beginning with *Hi* and an exclamation mark in any part of the message is not spam.
- ** Ivan? **. Mail beginning with *Ivan* personal address followed by any character is not spam.
- ** Ivan\? **. An email message containing the *Ivan?* phrase is a good email.

If characters * and ? are included into a phrase, then they should be preceded by the \ character to prevent their misrecognition in Anti-Spam. Then two characters are used instead of one: * and \?.

To create the list of allowed phrases:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it contains allowed phrases** box and click the **Select** button.

6. In the **List of allowed phrases** window that will open, click the **Add** link.

7. In the **Allowed phrase** window that will open, enter a line or a mask.

IMPORTING THE LIST OF ALLOWED SENDERS

Addresses in the list of allowed senders can be imported from **.txt*, **.csv* files, or from Microsoft Office Outlook / Microsoft Outlook Express address book.

To import the list of allowed senders:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Exact methods** tab, in the **Consider message as not spam** block, check the **If it is from allowed sender** box and click the **Select** button.

6. In the **List of allowed senders** window that will open, click the **Import** link.

7. Select the import source from the dropdown menu:

   - **Import from file**. After selection of this source a file selection dialog will be displayed. The application supports import from *.csv* or *.txt* file types.

   - **Import from the Address Book**. After selection of this source an address book selection dialog will be displayed. Select the required address book from this window.

DETERMINING SPAM AND POTENTIAL SPAM RATINGS

Experts at Kaspersky Lab work to provide the best possible precision of spam and probable spam detection in Anti-Spam.

Spam recognition is based on modern filtration methods, which allow training Anti-Spam to distinguish spam, probable spam and useful email. The training procedure is implemented as analysis of a certain number of user messages.

Anti-Spam is trained by working with the Training Wizard, and training from email clients. In doing so, every individual element of good emails or spam are assigned a factor. When an email message enters your inbox, Anti-Spam scans the message using the iBayes algorithm for elements of spam and of good email. The factors for each element are totaled, and the spam rating and potential spam rating are calculated.

Probable spam rating defines the value that will cause assignment of the *Probable spam* status to a message, if exceeded. If the **Recommended** Anti-Spam level is used, any message with spam rating higher than 60% is considered probable spam. Messages for which the rating value is less than 60%, are considered useful mail. You can modify the specified value.

Spam rating defines the value that will cause assignment of the *Spam* status to a message, if exceeded. Any message with rating value higher than the one specified will be perceived as spam. By default, the spam rating is 90% for the **Recommended** level. It means that any message with the rating higher than 90% will be marked as spam. You can modify the specified value.

To edit the set values of spam and probable spam ratings, perform the following steps:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Expert methods** tab, in the **Spam rate** block, fine-tune the spam and probable spam ratings.

SELECTING THE SPAM RECOGNITION ALGORITHM

Anti-Spam mail analysis is based on the selected recognition algorithms:

- **Heuristic analysis**. Anti-Spam analyzes messages using heuristic rules. Heuristic analysis is always enabled.
- **Image recognition (GSG technology)**. Anti-Spam uses GSG technology to detect graphic spam.
- **Analysis of attachments of RTF format**. Anti-Spam analyzes documents attached to messages checking them for spam signs.
- **Self-training text recognition algorithm (iBayes)**. The iBayes algorithm defines whether a message is spam or non-spam based on the frequency in the text of words characteristic of spam. You should train (see section "Training Anti-Spam" on page 115) the iBayes algorithm before you use it.

To enable / disable a specific spam recognition algorithm for analysis of email messages, perform the following steps:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Expert methods** tab, in the **Recognition algorithms** block, check / uncheck the corresponding boxes.

USING ADDITIONAL SPAM FILTERING FEATURES

Besides basic properties used to filter messages (lists of allowed and blocked senders, recognition algorithms, etc.), you can specify additional signs. Based on these features, a message will be assigned the *spam* status with a certain degree of probability.

To enable / disable individual additional spam filtration properties, perform the following steps:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.

4. Click the **Settings** button for the component you have selected.

5. In the window that will open, on the **Expert methods** tab, click the **Additional** button.

6. In the **Additional** window that will open, check / uncheck the box next to the required spam signs.

ADDING A LABEL TO MESSAGE SUBJECT

You can use the opportunity to add the **[!! SPAM]** or **[?? Probable Spam]** labels to the **Subject** field of the messages, which will be recognized as spam or probable spam after check.

To enable / disable addition of labels to the message subjects, perform the following steps:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the **Additional** window that will open, check / uncheck the appropriate boxes in the **Actions** section. You can edit the text of the label.

FILTERING EMAIL MESSAGES AT THE SERVER. MAIL DISPATCHER

You can view the list of email messages on the server without downloading them to your computer. The opportunity allows you to reject some messages saving time and traffic while working with email and also decreasing the risk of downloading spam or viruses to your computer.

Mail Dispatcher is used to manage the messages residing on the server. Mail Dispatcher window opens every time before mail retrieval provided it is enabled.

Mail Dispatcher opens only when mail is received via POP3 protocol. Mail Dispatcher does not appear if your POP3 server does not support viewing of email headers or all messages on server are from the addresses included into the list of allowed senders.

The list of email messages residing on the server is displayed in the central part of the Dispatcher window. Select the message in the list for a detailed analysis of its header. Header viewing may be useful, for example, in this situation: spammers install a malicious program on your colleague's computer; this program sends spam with his name on it, using his mail client's contact list. The probability that your address is present in the contact list of your colleague is quite high. Certainly it will result in lots of spam sent to your mailbox. In such cases you cannot determine if a message has been sent by your colleague or spammer using the sender address only. That is why email headers should be checked. It is recommended to check who and when has sent a message and also note its size. When possible, track the message route from sender to your email server – relevant information should be available in the email header. All this information should be contained in the email headers. These steps allow you to decide if a message really should be downloaded from server or it is safer to delete it.

To use Mail Dispatcher:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Additional** tab, in the **Incoming messages** block, check the **Open Mail Dispatcher when receiving email through POP3 protocol** box.

In order to delete messages from the server using Mail Dispatcher:

1. In the Dispatcher window, check the box next to the message in the **Delete** column.
2. Click the **Delete selected** button in the top part of the window.

Messages will be deleted from the server. You will receive a notification marked as **[!! SPAM]** and processed according to the rules set for your mail client.

EXCLUDING MICROSOFT EXCHANGE SERVER MESSAGES FROM THE SCAN

You can exclude from anti-spam scanning, email messages which originate within the internal network (for example, corporate mail). Please note that messages will be considered as internal mail, if Microsoft Office Outlook is used on all network computers and user mailboxes are located on the same Exchange server or on servers linked via X400 connectors.

By default, the Anti-Spam component does not scan Microsoft Exchange Server messages.

If you wish Anti-Spam to analyze the messages:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. Click the **Settings** button for the component you have selected.
5. In the window that will open, on the **Additional** tab, in the **Exclusions** block, uncheck the **Do not check Microsoft Exchange Server native messages** box.

ACTIONS TO BE PERFORMED ON SPAM

If after scanning you find that an email is spam or probable spam, further operations of Anti-Spam depend on the status of the object and the action selected. By default, email messages considered **spam** or probable spam, are modified: in the Subject field of the message, the **[!! SPAM]** or **[?? Probable Spam]** label is added, respectively.

You can select additional actions to be taken on spam or probable spam. To do so, in Microsoft Office Outlook (see section "Configuring spam processing in Microsoft Office Outlook" on page 127) and Microsoft Outlook Express (Windows Mail) (see section "Configuring spam processing in Microsoft Outlook Express (Windows Mail)" on page 129) clients, special plug-ins are provided. You can configure filtration rules for The Bat! (see section "Configuring spam processing in The Bat!" on page 129) and Thunderbird (see section "Configuring spam processing in Thunderbird" on page 130) mail clients.

SEE ALSO:

CONFIGURING SPAM PROCESSING IN MICROSOFT OFFICE OUTLOOK

The spam processing settings window automatically opens the first time you run Microsoft Outlook after installing Computer Protection.

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field.

You can assign the following processing rules for both spam and probable spam:

- **Move to folder –** spam is moved to the folder of your inbox that you specify.
- **Copy to folder –** a copy of the email message is created and moved to the specified folder. The original email is saved in your **Inbox**.
- **Delete –** delete spam from the user's mailbox.
- **Skip –** leave the email in the **Inbox** folder.

To do so, select the appropriate value from the dropdown list in the **Spam** or **Probable spam** section.

When training Anti-Spam with mail client (see section "Training using email client" on page 117), a marked message will be sent to Kaspersky Lab as a spam sample. Click the **Additionally after manually marking emails as spam** link to select the spam sample transfer mode in the window that will open. Click the **Additionally after manual marking emails as not spam** link to select the mode of sending not spam samples (i.e. samples mistakenly considered as spam earlier).

Furthermore, you can select the algorithm for common operation of Microsoft Office Outlook and Anti-Spam plug-in:

- **Scan upon receiving**. All emails that enter the user's inbox are initially processed according to the Microsoft Office Outlook rules. After processing is complete, the remaining messages that do not fall under any of the rules are processed by the Anti-Spam plug-in. In other words, emails are processed according to the priority of the rules. Sometimes the priority sequence may be ignored, if, for example, a large number of emails arrive in your inbox at the same time. As a result, situations could arise when information about an email processed by a Microsoft Office Outlook rule is logged in the Anti-Spam report marked with the *spam* status. To avoid this, we recommend configuring the Anti-Spam plug-in as a Microsoft Office Outlook rule.
- **Use Microsoft Office Outlook rule**. With this option, incoming messages are processed using the hierarchy of Microsoft Office Outlook rules, one of which must be a rule about Anti-Spam processing emails. This is the best configuration, as it does not cause conflicts between Microsoft Outlook and the Anti-Spam plug-in. The only shortcoming of this arrangement is that you should create and delete spam processing rules through Microsoft Office Outlook manually.

To create a spam processing rule:

1. Run Microsoft Office Outlook and use the **Tools** → **Rules and Alerts** command in the main application menu. The method used to access the wizard depends upon your version of Microsoft Office Outlook. This Help file describes how to create a rule using Microsoft Office Outlook 2003.
2. In the **Rules and Alerts** window that will open, on the **Email Rules** tab click the **New Rule** button. As a result, the Rules Wizard will be launched. Rules Wizard includes the following steps:
   a. You should decide whether you want to create a rule from scratch or using a template. Select the **Start from a blank rule** option and select the **Check messages when they arrive** scan condition. Click the **Next** button.
   b. Click the **Next** button in the message filtering condition configuration window without checking any boxes. Confirm in the dialog box that you want to apply this rule to all emails received.
   c. In the window for selecting actions to apply to messages, check the **perform a custom action** box in the action list. In the lower part of the window, click the **a custom action** link. Select Kaspersky Anti-Spam from the drop-down list in the window that will open and click the **OK** button.
   d. Click the **Next** button in the exclusions from the rules window without checking any boxes.
   e. In the final window, you can change the rule's name (the default name is Kaspersky Anti-Spam). Make sure that the **Turn on this rule** box is checked, and click the **Finish** button.
3. The default position for the new rule is first on the rule list in the **Rules and Alerts** window. If you like, move this rule to the end of the list so it is applied to the email last.

All incoming emails are processed with these rules. The order in which the program applies the rules depends on the priority you assign to each rule. The rules are applied from the beginning of the list. Each subsequent rule is ranked lower than the previous one. You can change the priority for applying rules to emails.

If you do not want the Anti-Spam rule to further process emails after a rule is applied, you must check the **Stop processing more rules** box in the rule settings (see Step 3 in creating a rule).

If you are experienced in creating email processing rules in Microsoft Outlook, you can create your own rule for Anti-Spam based on the algorithm that we have suggested.

The spam and probable spam processing settings for Microsoft Office Outlook are displayed on the special **Anti-Spam** tab of the **Tools** → **Options** menu item.

CONFIGURING SPAM PROCESSING IN MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

The spam processing settings window opens when your run your client after the installation of the application.

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field.

You can assign the following processing rules for both spam and probable spam:

- **Move to folder –** spam is moved to the folder of your inbox that you specify.
- **Copy to folder –** a copy of the email message is created and moved to the specified folder. The original email is saved in your **Inbox**.
- **Delete –** delete spam from the user's mailbox.
- **Skip –** leave the email in the Inbox folder.

To define the required processing rule, select the appropriate value from the dropdown list in the **Spam** or **Probable spam** section.

When training Anti-Spam with mail client (see section "Training using email client" on page 117), a marked message will be sent to Kaspersky Lab as a spam sample. Click the **Additionally after manually marking emails as spam** link to select the spam sample transfer mode in the window that will open. Click the **Additionally after manual marking emails as not spam** link to select the mode of sending not spam samples (i.e. samples mistakenly considered as spam earlier).

The window used for configuration of spam processing methods can be opened by clicking the **Settings** button next to other Anti-Spam buttons in the task bar: **Spam** and **Not Spam**.

CONFIGURING SPAM PROCESSING IN THE BAT!

Actions on spam and probable spam in The Bat! are defined by the client's own tools.

To set up spam processing rules in The Bat!, please do the following:

1. In the **Properties** menu of the mail client, select **Settings**.
2. Select the **Spam protection** item from the settings tree.

Displayed settings of anti-spam protection apply to all installed Anti-Spam modules that support integration with The Bat!.

You need to define the rating level and specify how messages with certain rating should be handled (in case of Anti-Spam – the probability of message being spam):

- delete messages with the rating that exceeds the specified value;

- move email messages with a given rating to a special spam folder;
- move spam marked with special headers to the spam folder;
- leave spam in the **Inbox** folder.

After processing an email, Computer Protection assigns a spam or probable spam status to the message based on a rating with an adjustable value. The Bat! has its own email rating algorithm for spam, also based on a spam rating. To prevent discrepancies between spam rating in Computer Protection and The Bat!, all messages checked in Anti-Spam are assigned the rating corresponding to the message status: Not Spam email – 0%, Probable spam – 50%, Spam – 100%. Thus, the email rating in The Bat! corresponds to the rating of the corresponding status and not to the email rating assigned in Anti-Spam.

For more details on the spam rating and processing rules, see documentation for The Bat!.

CONFIGURING SPAM PROCESSING IN THUNDERBIRD

By default, email messages classified by Anti-Spam as spam or probable spam are marked with special labels **[!! SPAM]** or **[?? Probable Spam]** in the **Subject** field. To perform actions with such messages in Thunderbird, use the rules from the **Tools** → **Message Filters** menu (for more details about using the mail client please refer to Mozilla Thunderbird Help).

Thunderbird's Anti-Spam plug-in module allows training based on messages received and sent using this email client application and checking your email correspondence for spam at the server. The plug-in module is integrated into Thunderbird and forwards messages to the Anti-Spam component for scanning when the **Tools** → **Run anti-spam filters in folder** menu command is being executed. This way, Computer Protection checks messages instead of Thunderbird. This does not alter the functionality of Thunderbird.

The Anti-Spam plug-in module status is displayed as an icon in the Thunderbird status line. The grey color of the icon informs the user that a problem has occurred in the plug-in operation, or that the Anti-Spam (see page 113) component is disabled. Double-clicking the icon opens the Computer Protection settings configuration window. To access the **Anti-Spam** configuration settings, click the **Settings** button in the **Anti-Spam** section.

RESTORING DEFAULT ANTI-SPAM SETTINGS

When configuring Anti-Spam, you are always able to restore its recommended settings. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

To restore default Anti-Spam settings, please do the following:

1. Open the main application windowand click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Spam** component.
4. In the **Security level** section, click the **Default level** button for the component selected.

ANTI-BANNER

Anti-Banner blocks advertising information located on banners built into interfaces of various programs installed on your computer, or displayed online.

Not only are banner ads devoid of useful information but they also distract you from your work and increase the amount of traffic on your computer. Anti-Banner blocks the commonest types of banners that are currently known, using masks which are included in the Computer Protection installation package. You can disable banner blocking or create your own lists of allowed and blocked banners.

Kaspersky Lab specialists have compiled a banner ad mask list based on specially conducted research and have included it with the Computer Protection installation package. Banner ads, which match the masks on the list, will be blocked by Anti-Banner unless banner blocking is disabled. To block banners with address masks not found in the standard list, the heuristic analyzer is used (see section "Using heuristic analysis" on page 131).

Besides that, you can create white (see section "Creating the list of allowed banner addresses" on page 132) and black (see section "Creating the list of blocked banner addresses" on page 132) lists of banners to determine whether a banner should be allowed or blocked.

After Computer Protection is installed, Anti-Banner is disabled.

To edit Anti-Banner settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.
4. Make the required changes in the settings for the component you have selected.

IN THIS SECTION:

USING HEURISTIC ANALYSIS

Banners, which addresses are not included in the standard list can be scanned using heuristic analyzer. If it is in use, Computer Protection will analyze the images being downloaded for features typical of banners. Based on such analysis, the image may be identified as a banner and blocked.

To begin using heuristic analyzer:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.

4. In the **Scan methods** section, check the **Use heuristic analyzer** box for the component selected.

ADVANCED COMPONENT SETTINGS

Kaspersky Lab specialists have compiled a banner ad mask list based on specially conducted research and have included it with the Computer Protection installation package. Banner ads, which match the masks on the list, will be blocked by Anti-Banner unless banner blocking is disabled.

When creating the lists of allowed / banned banners, either banner's IP address or its symbol name (URL) may be entered. To avoid dubbing, you can use an advanced option which allows converting IP addresses into domain names, and vice-versa.

To disable the use of the banner list included in the Computer Protection installation package:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.
4. In the **Scan methods** section, uncheck the **Use common banner list** box for the component selected.

To use the option of converting banners' IP addresses into domain names (or domain names into IP addresses), please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.
4. In the **Scan methods** section, check the **Resolve IP addresses to domain names** box for the component selected.

CREATING THE LIST OF ALLOWED BANNER ADDRESSES

A user creates the "white" list of banners while working with Computer Protection if certain banners should not be excluded. This list contains the masks for allowed banner ads.

To add a new mask to the white list, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.
4. In the **Additional** section, check the **Use White list of addresses** box for the component selected, and click the **Settings** button.
5. In the **"White" list** window that will open, click the **Add** link.
6. Enter a mask of an allowed banner in the **Address mask (URL)** window that will open. To stop using a mask, you do not have to delete it from the list; unchecking the box next to it renders it inactive.

CREATING THE LIST OF BLOCKED BANNER ADDRESSES

You can create a list of banned banner addresses, which will be blocked by Anti-Banner when detected.

To add a new mask to the black list, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.
4. In the **Additional** section, check the **Use Black list of addresses** box for the component selected, and click the **Settings** button.
5. In the **"Black" list** window that will open, click the **Add** link.
6. Enter a mask of blocked banner in the **Address mask (URL)** window that will open. To stop using a mask that you created, you do not have to delete it from the list; unchecking the box next to it renders it inactive.

EXPORTING / IMPORTING BANNER LISTS

You can copy the lists of allowed / banned banners you have created from one computer to another. While exporting the list, you can copy either the selected list element only, or the entire list. While importing the list, you can choose to add the new addresses to the existing list, or replace the existing list with the one being imported.

To copy the created lists of allowed / banned banners, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section select the **Anti-Banner** component.
4. In the **Additional** section, click the **Settings** button for the list that should be copied, for the component selected.
5. In the **"White" list** (or **"Black" list**) window that will open, use the **Import** or **Export** links.

COMPUTER SCAN

Scanning the computer for viruses and vulnerabilities is one of the most important tasks in ensuring the computer's security. The virus scan detects the spreading of malicious code, which has not been detected by the malware protection for some reasons. Vulnerability scan detects software vulnerabilities that can be used by intruders to spread malicious objects and obtain access to personal information.

Kaspersky Lab distinguishes virus scan tasks (see page 134), including scan of removable drives (see page 140), and system's and applications' vulnerability scan (see page 144).

In order to change the settings of any scan task:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**, **Vulnerability Scan**) section.
3. Make the required changes in the settings for the task selected.

IN THIS SECTION:

VIRUS SCAN

Kaspersky Lab specialists distinguish several types of virus scan tasks:

- **Objects Scan**. Objects, selected by the user, are scanned. Any object of the computer's file system can be scanned. Within this task you can configure the settings for scanning removable drives.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Operating system startup objects are scanned.

The Full Scan and Quick Scan tasks are specific tasks. It is not recommended to change the list of objects scanned by these tasks.

Each scan task is performed in the specified area and can be launched according to the schedule created. A set of virus scan task parameters define the security level. By default, three levels are provided.

After the virus scan task starts, its progress is displayed in the **Scan My Computer** section of the Computer Protection main window, in the field under the name of the started task. If a threat is detected, the application performs the specified action.

When searching for threats, information on the results is logged in a report of Computer Protection.

In addition, you can select an object to be scanned for viruses with the standard tools of the Microsoft Windows operating system, for example, in the **Explorer** program window or on your **Desktop**, etc. Place the cursor on the desired object's name, right-click to open the Microsoft Windows context menu, and select the **Scan for viruses** option.

Figure 12. Microsoft Windows context menu

You can also view the scan report containing full information about events, which have occurred during the execution of the task.

SEE ALSO:

STARTING THE VIRUS SCAN TASK

A virus scan task can be started in one of the following ways:

- from the Computer Protection context menu (see section "Context menu" on page 50);
- from the Computer Protection main window (see section "My Computer Protection" on page 53);
- using an existing shortcut (see page 137).

Task execution information will be displayed in the main window of My Computer Protection.

In addition, you can select an object to be scanned with the help of standard tools of the Microsoft Windows operating system (for example, in the **Explorer** program window or on your **Desktop**, etc.).

Figure 13. Microsoft Windows context menu

To start the task using a shortcut:

1. Open the folder in which a shortcut was created.
2. Start the task by double-clicking a shortcut. Task execution progress will be displayed in the main window of My Computer Protection, in the **Scan My Computer** section.

To start a virus scan task from the application context menu:

1. Right-click the application icon in the taskbar notification area.
2. Select the **Virus Scan** item in the context menu that will open.
3. In the main window of My Computer Protection that opens, in the **Scan My Computer** section, click the button with the name of the required task.

To start the full scan of the computer, select the **Full Scan** item from the context menu. This will start a full computer scan. Task execution progress will be displayed in the main window of My Computer Protection, in the **Scan My Computer** section.

To start the virus scan task from the main application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the button with the name of the required task on it.

To start a virus scan task for a selected object from the Microsoft Windows context menu:

1. Right-click thename of the selected object.
2. Select the **Virus Scan** item in the context menu that will open. The progress and the results of the task execution will be displayed in the window that will open.

CREATING A SHORTCUT FOR TASK EXECUTION

The application provides the option of creating shortcuts for a quick start of full scan tasks and quick scan tasks. This allows starting the required scan task without opening the main application window or the context menu.

To create a shortcut for scan task start, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Scan My Computer** section.
3. In the right part of the window, in the **Scan tasks quick run** block, click the **Create shortcut** button next to the name of the required task (**Quick Scan** or **Full Scan**).
4. Specify the path for saving a shortcut and its name in the window that will open. By default, the shortcut is created with the name of a task in the *My Computer* folder of the current computer user.

CREATING A LIST OF OBJECTS TO SCAN

Each virus scan task has its own default list of objects. These objects may include items in the computer's file system, such as logical drives and **email databases**, or other types of objects such as network drives. You can edit this list.

Objects will appear on the list immediately you add them. If the **Include subfolders** box has been selected when adding the object, the scan will run recursively.

To delete an object from the list, select the object and click the **Delete** link.

Objects which appear on the list by default cannot be edited or deleted.

In addition to deleting objects from the list, you can also temporarily skip them when running a scan. To do so, select the object from the list and uncheck the box to the left of the object's name.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started!

To create a list of objects for an object scan task, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the **Add** link.
4. In the **Select object to scan** window that will open, select an object and click the **Add** button. Click the **OK** button after you have added all the objects you need. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

To create the list of objects for quick scan or full scan tasks, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the left part of the window, select the **Full scan** (**Quick scan**) task.
3. In the **Scan scope** block, click the **Settings** button for the task selected.
4. In the **<Scan task name>: list of objects** window that will open, create a list using the **Add**, **Edit**, **Delete** links. To exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

CHANGING SECURITY LEVEL

The security level is a preset collection of scan settings. Kaspersky Lab's specialists distinguish three security levels. You should make the decision on which level is to select, based on your own preferences. You can select one of the following security levels:

- **High**. It should be enabled if you suspect that your computer has a high chance of becoming infected.
- **Recommended**. This level is suitable in most cases, and is recommended for using by Kaspersky Lab specialists.
- **Low**. If you are using applications requiring considerable RAM resources, select the Low security level because the application puts least demand on system resources in this mode.

If none of the preset levels meet your needs, you can configure the scan settings yourself. As a result, the security level's name will be changed to **Custom**. To restore the default scan settings, select one of the preset security levels.

To change the defined security level, perform the following actions:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
4. In the **Security level** section, set the required security level for the task selected.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If a threat is detected, Computer Protection assigns it one of the following statuses:

- malicious program (such as, a *virus* or a *Trojan*);
- *potentially infected* status when the scan cannot determine if the object is infected. This is caused when the application detects a sequence of code in the file from an unknown virus, or modified code from a known virus.

If Computer Protection detects infected or potentially infected objects when scanning for viruses, it will notify you about it. You should react to an emerging threat by selecting an action to be performed on the object. Computer Protection selects the **Prompt for action** option as the action on a detected object which is the default setting. You can change the action. For example, if you are sure that each detected object should be attempted to disinfect, and do not want to select the **Disinfect** action each time you receive a notice about the detection of an infected or suspicious object, select the following action: **Do not prompt. Disinfect**.

Before attempting to disinfect or delete an infected object, Computer Protection creates a backup copy of it to allow later restoration or disinfection.

If you work in automatic mode (see section "Step 3. Selecting protection mode" on page 41), Computer Protection will automatically apply the action recommended by Kaspersky Lab specialists when dangerous objects are detected. For malicious objects this action is **Disinfect. Delete if disinfection fails**, for suspicious objects – **Skip**.

To change the specified action to be performed on detected objects:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Action** block, specify the required action for the task selected.

CHANGING THE TYPE OF OBJECTS TO SCAN

When specifying the type of objects to scan, you establish which file formats and sizes will be scanned when the selected scan task runs.

When selecting the file type, you should remember the following features:

- Probability of penetration of malicious code into several file formats (such as *.txt*) and its further activation is quite low. At the same time, there are formats that contain or may contain an executable code (such as *.exe*, *.dll*, *.doc).* The risk of penetration and activation of malicious code in such files is fairly high.

- Remember that an intruder can send a virus to your computer in a file with the *.txt* extension, whereas it is in fact an executable file renamed as *.txt* file. If you have selected the **Files scanned by extension** option, such a file will be skipped by the scan. If the **Files scanned by format** option has been selected, the file protection will analyze the file header and may determine that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

To change the type of scanned objects:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
4. In the **Security level** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Scope** tab, in the **File types** block, select the required settings.

SCAN OPTIMIZATION

You can shorten the scan time and increase the operating speed of Computer Protection. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

Besides, you can restrict the duration of scan for one file. Once the specified time elapses, the scan is stopped.

To scan only new and changed files:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
4. In the **Security level** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Scope** tab, in the **Scan optimization** block, check the **Scan only new and changed files** box.

To impose a time restriction on the scan duration:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Security level** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Scope** tab, in the **Scan optimization** block, check the **Skip files scanned longer than** box and specify the scan duration in the field next to it.

SCANNING REMOVABLE DISK DRIVES

Nowadays, malicious objects using operating systems' vulnerabilities to replicate via networks and removable media have become increasingly widespread.

Use the option of scanning removable drives when connecting them to the computer. To do so, you have to select one of the actions to be performed by Computer Protection:

- **Do not scan**. Removable drives are not scanned automatically when being connected to the computer.
- **Ask User**. By default, Computer Protection prompts the user for further action when a removable drive is being connected.
- **Full Scan**. When connecting removable drives, the application performs a full scan of files stored on them, according to the Full Scan task's settings.
- **Quick Scan**. When connecting removable drives, the application scans all files according to the Quick Scan task's settings.

To use the functionality for scanning of removable media at connection, perform the following steps:

1. Open the mainapplication window and click the **Settings** link in the top part of the window.

2. In the left part of the window, select the **Scan My Computer** section.

3. In the **Scan removable drives on connection** block, select the action and define the maximum size of a drive to scan in the field below, if necessary.

SCAN OF COMPOUND FILES

A common method of concealing viruses is to embed them into compound files: archives, databases, etc. To detect viruses that are hidden this way a compound file should be unpacked, which can significantly lower the scan speed.

For each type of compound file, you can select to scan either all files or only new ones. To do so, use the link next to the name of the object. It changes its value when you left-click on it. If you select the mode of scanning new and changed files only (see page 139), you will not be able to select which types of compound files are to be scanned.

You can restrict the maximum size of the compound file being scanned. Compound files with the size larger than the specified value will not be scanned.

Large files extracted from archives will be scanned even if the **Do not unpack large compound files** box is checked.

To modify the list of scanned compound files:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Security level** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Scope** tab, in the **Scan of compound files** block, select the required type of compound files to be scanned.

In order to set the maximum size of compound files to be scanned:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Security level** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Scope** tab, in the **Scan of compound files** block, click the **Additional** button.

6. In the **Compound files** window that will open, check the **Do not unpack large compound files** box and specify the file size in the field below.

SCAN TECHNOLOGY

Additionally you can specify the technology which will be used during the scan. You can select one of the following technologies:

- **iChecker**. This technology can increase scan speed by excluding certain objects from the scan. An object is excluded from the scan using a special algorithm that takes into account the release date of the application database, the date the object was last scanned and any modifications to the scan settings.

  For example, you have an archive file with the *not infected* status assigned to it by Computer Protection following a scan. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If the archive's structure has changed because a new object has been added to it, or if the scan settings have changed, or if the application databases have been updated, the application will re-scan the archive.

  There are limitations to iChecker: it does not work with large files and applies only to the objects with a structure that the application recognizes (for example, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **iSwift**. This technology is a development of the iChecker technology for computers using an NTFS file system. There are limitations to iSwift: it is bound to a specific file location in the file system and can apply only to objects in NTFS.

To change the object scan technology:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Security level** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Additional** tab, in the **Scan technologies** block, select the required setting value.

CHANGING THE SCAN METHOD

You can edit the scan settings which determine its thoroughness. By default, the mode of using application's database records to search for threats is always enabled. Moreover, you can apply various scan methods and scan technologies (see page 141).

The scan mode in which Computer Protection compares the object found to the database records is called *signature analysis*, and is always used by default. Additionally, you can always use the *heuristic analysis*. This method presumes the analysis of the actions an object performs within the system. If its actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious.

Additionally you can select the detail level for heuristic analysis: **light**, **medium**, or **deep**. To do so, move the slider bar to the selected position.

Apart from these scan methods, you can also use the rootkit scan. Rootkits are sets of tools that can hide malicious programs in your operating system. These utilities are injected into the system, hiding their presence and the presence of processes, folders and the registry keys of other malicious programs installed with the rootkit. If the scan is enabled, you can specify detailed level (advanced analysis) to detect rootkits, which will scan carefully for these programs by analyzing a large number of various objects.

To specify which scan method to use:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Additional** tab, in the **Scan methods** block, select the required values for the settings.

RUN MODE: CREATING A SCHEDULE

You can create a schedule to start virus scan tasks automatically.

The main thing to choose is the time interval between task startups. To change the frequency, specify the schedule settings for the selected option.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the task to start automatically as soon as it becomes possible.

To edit a schedule for scan tasks:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Run mode** tab, in the **Schedule** block, select the **Manually** option if you wish to start the scan task at the most suitable time. If you wish the task to run periodically, select **By schedule** and create a task launch schedule.

To configure automatic launches of skipped tasks:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Run mode** tab, in the **Schedule** block, check the **Run skipped tasks** box.

RUN MODE: SPECIFYING AN ACCOUNT

You can specify an account used by the application when performing a virus scan.

To specify an account:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Run mode** tab, in the **User account** block, check the **Run task as** box. Specify the user name and password.

FEATURES OF SCHEDULED TASK LAUNCH

All scan tasks can be started manually, or by a schedule.

Scheduled tasks feature an additional functionality, for example, you can *pause scheduled scan if the screensaver is inactive, or the computer is unlocked*. This functionality postpones the task launch until the user has finished working on the computer. So, the scan task will not take up system resources during the work.

To launch scan tasks only when the computer isn't in use any more, please do the following:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Run mode** block, click the **Settings** button for the task selected.

5. In the window that will open, on the **Run mode** tab, in the **Schedule** block, check the **Pause scheduled scan when screensaver is inactive or computer is unlocked** box.

RESTORING DEFAULT SCAN SETTINGS

When configuring task settings, you can always restore the recommended ones. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

In order to restore the default file scan settings:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the left part of the window, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**) section.

4. In the **Security level** block, click the **Default level** button for the task selected.

VULNERABILITY SCAN

Vulnerability scan task consists in system security diagnostics and search for potential vulnerabilities usually used by intruders to do harm to computers.

When scanning vulnerabilities, the application analyzes the system, and searches for anomalies and damages in the operating system's and browser's settings. Security diagnostics has many dimensions, including: searching for Rootkit installations (i.e. programs for secretly monitoring a hacked system), searching for vulnerable services and settings, and gathering information about processes and drivers.

System diagnostics for vulnerabilities may take some time. When it is complete, collected information will be analyzed to evaluate security problems from the perspective of a possible threat to the system.

All the problems detected at the system analysis stage will be grouped based on the degree of danger it poses. Kaspersky Lab offers a set of actions for each group of problems which help eliminate vulnerabilities and weak points in the system's settings. There are three groups of problems distinguished, and, respectively, three groups of actions associated with them:

- *Strongly recommended actions* will help eliminate problems posing a serious security threat. You are advised to perform all actions of this group.

- *Recommended actions* help eliminate problems posing a potential threat. You are advised to perform all actions of this group too.

- *Additional actions* help repair system damages which do not pose a current threat but may threat the computer's security in the future.

The outcome of the search for potential vulnerabilities in the operating system and in installed user applications is represented by direct links to critical fixes (application updates).

After the vulnerability scan task starts (see page 145), its progress is displayed in the main application window and in the **Vulnerability Scan** window, in the **Finish** field. Vulnerabilities detected when scanning the system and applications, are displayed in the same window, on the **System vulnerabilities** and **Vulnerable applications** tabs.

When searching for threats, information on the results is logged in a report of Computer Protection.

In the **Vulnerability Scan** section in the application settings window, you can set a start schedule (see page 146) and create a list of objects to be scanned for a vulnerability scan task (see page 145), similarly to virus scan tasks. By default, the applications already installed on the computer are selected as scan objects.

SEE ALSO:

STARTING THE VULNERABILITY SCAN TASK

The vulnerability scan task can be started in the following ways:

- from the Computer Protection main window (see section "My Computer Protection" on page 53);
- using an existing shortcut (see page 145).

Task execution information will be displayed in the main window of My Computer Protection and in the **Vulnerability Scan** window.

To start the task using a shortcut:

1. Open the folder in which a shortcut was created.
2. Start the task by double-clicking a shortcut. The task progress will be displayed in the main application window.

To start the vulnerability scan task from the application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan My Computer** section.
3. Click the **Open Vulnerability Scan window** button.
4. In the window that will open, click the **Start Vulnerability Scan** button. Task execution progress will be displayed in the **Finish** field. Click the button again to stop the task execution.

CREATING A SHORTCUT FOR TASK EXECUTION

The application provides the option of creating a shortcut for a quick start of vulnerability scan task. This allows starting the task without opening the main application window.

To create a shortcut for starting the vulnerability scan task:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the left part of the window, select the **Scan My Computer** section.
3. In the right part of the window, in the **Scan tasks quick run** section, click the **Create shortcut** button next to the name of the task (**Vulnerability Scan**).
4. Specify the path for saving a shortcut and its name in the window that will open. By default, the shortcut is created with the name of a task in the *My Computer* folder of the current computer user.

CREATING A LIST OF OBJECTS TO SCAN

Vulnerability scan task has its own default list of objects to scan. These objects include operating system and programs, installed on your computer. You can also specify additional objects to scan: objects of the computer's file system (for example, logical drives, **Email databases**), or other types of objects (for example, network drives).

Objects will appear on the list immediately you add them. If the **Include subfolders** box has been selected when adding the object, the scan will run recursively. Manually added objects will be also scanned for viruses.

To delete an object from the list, select the object and click the **Delete** link.

Objects which appear on the list by default cannot be edited or deleted.

In addition to deleting objects from the list, you can also temporarily skip them when running a scan. To do so, select the object from the list and uncheck the box to the left of the object's name.

If the scan scope is empty, or it contains no selected objects, a scan task cannot be started!

To create the list of objects for a vulnerability scan task:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
4. In the **Scan scope** block, click the **Settings** button for the task selected.
5. In the **Vulnerability Scan: list of objects** window that will open, create a list using the **Add**, **Edit**, **Delete** links. To temporarily exclude any objects from the list of objects to be scanned, uncheck the boxes next to them.

RUN MODE: CREATING A SCHEDULE

Vulnerability scan task can be scheduled to run automatically.

The main thing to choose is the time interval between task startups.

If it is not possible to start the task for any reason (for example, the computer was not on at that time), you can configure the task to start automatically as soon as it becomes possible.

To edit a schedule for scan tasks:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Run mode** tab, in the **Schedule** block, select the **Manually** option if you wish to start the scan task at the most suitable time. If you wish the task to run periodically, select **By schedule** and create a task launch schedule.

To configure automatic launches of skipped tasks:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Run mode** tab, in the **Schedule** block, check the **Run skipped tasks** box.

RUN MODE: SPECIFYING AN ACCOUNT

You can specify an account used by the application when performing a vulnerability scan.

To specify an account:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the left part of the window, select the **Vulnerability Scan** task in the **Scan My Computer** section.
4. In the **Run mode** block, click the **Settings** button for the task selected.
5. In the window that will open, on the **Run mode** tab, in the **User account** block, check the **Run task as** box. Specify the user name and password.

Update

Keeping the application updated is a prerequisite for reliably protecting your computer. New viruses, Trojans, and malicious software emerge daily, so it is important to update the application regularly to keep your personal data constantly protected. Information about threats and methods of their neutralization is stored in Computer Protection databases, therefore their timely updating is an essential part in the maintenance of reliable protection.

Application update downloads and installs the following updates on your computer:

- Computer Protection databases.

  The protection of information is based on databases which contain signatures of threats and network attacks, and the methods used to fight them. Protection components use these databases to search for and disinfect dangerous objects on your computer. The databases are added to every hour with records of new threats. Therefore, you are advised to update them on a regular basis.

  In addition to the Computer Protection databases, the network drivers that enable the application's components to intercept network traffic are also updated.

- Application modules.

  In addition to Computer Protection databases, you can also update program modules. The update packages fix Computer Protection vulnerabilities and add new or improve the existing functionality.

Kaspersky Lab's update servers is the primary source of updates for Computer Protection.

To successfully download updates from servers, your computer must be connected to the Internet. By default, the Internet connection settings are determined automatically. If the proxy server is not properly configured automatically, the connection settings (see page 150) can be modified manually.

During an update, the application modules and databases on your computer are compared with those at the update source. If your computer has the latest version of the databases and application modules, you will see a notification window confirming that your computer's protection is up to date. If the databases and modules on your computer differ from those on the update server, the application downloads only the incremental part of the updates. The fact that not all the databases and modules are downloaded significantly increases the speed of copying files and saves Internet traffic.

If the databases are outdated, the update package can be large and it can cause the additional internet traffic (up to several tens of Mb).

Prior to updating the databases Computer Protection creates their backup copies in case you may want to roll back to the previous database version.

You might need the update rollback (see page 149) option if, for example, the databases have become corrupted during the update process. You can easily roll back to the previous version and try to update the databases again.

You can copy the retrieved updates (see page 151) to a local source while updating Computer Protection. This service allows updating the databases and program modules on network computers to save Internet traffic.

You can also configure automatic update startup.

The **My Update Center** section of the main application window displays information about the current status of Computer Protection databases:

- release date and time;
- number of database records and their composition;
- databases status (up to date, out of date or corrupted).

You can view the update report, which contains full information about events that have occurred during the update task execution (the **Report** link in the upper part of the window). You can also see the virus activity overview at www.kaspersky.com by clicking the **Virus activity review** link.

IN THIS SECTION:

STARTING UPDATE

You can start updating Computer Protection at any time. Updates are downloaded from the selected update source.

You can update Computer Protection in one of the two following ways:

- from the context menu (see section "Context menu" on page 50);
- from the main application window (see section "My Computer Protection" on page 53).

Update information will be displayed in the **My Update Center** section of the main application window.

To start Computer Protection update from the context menu:

1. In the taskbar notificationarea, right-click the application icon.
2. Select the **Update** item from the dropdown menu.

To start Computer Protection update from the main application window:

1. Open the main application window.
2. In the window that will open, select the **Protection** section.
3. In the window that will open, select the **Update** section and click the **Start update** button.

ROLLING BACK THE LAST UPDATE

At the start of the update process, the application creates a backup copy of the current databases and modules. This allows the application to continue working, using the previous databases, if the update fails.

The rollback option is useful if, for example, part of the databases has been corrupted. Local databases may be corrupted by the user or by a malicious program, which is possible only if the Kaspersky PURE's self-defense (see page 248) is disabled. You can easily roll back to the previous databases and try to update the databases later.

To roll back to the previous database version:

1. Open the main application window.
2. In the window that will open, select the **My Computer Protection** section.
3. In the window that will open, select the **Update** section and click the **Roll back** button.

SELECTING UPDATE SOURCE

Update source is a resource containing updates for databases and application modules of Computer Protection. Update sources can be HTTP or FTP servers, or local or network folders.

The main update source is Kaspersky Lab's update servers. These are special Internet sites which contain updates for databases and application modules for all Kaspersky Lab products.

If you do not have access to Kaspersky Lab's update servers (for example, your computer is not connected to the Internet), you can call the Kaspersky Lab main office at +7 (495) 797-87-00 or +7 (495) 645-79-39 to request contact information of Kaspersky Lab partners who can provide you with updates on floppy disks or ZIP disks.

You can copy the updates from a removable disk and upload them to an FTP or HTTP site or save them in a local or network folder.

When ordering updates on removable media, please specify whether you also require updates for the application modules.

By default, the list of update sources contains only Kaspersky Lab's update servers.

If you select a resource outside the LAN as an update source, you must have an Internet connection to update.

If several resources are selected as update sources, Computer Protection will try to connect to them one after another, starting from the top of the list, and will retrieve the updates from the first available source.

To choose an update source:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. Select the **My Update Center** section in the left part of the window.
4. Click the **Settings** button in the **Update source** section.
5. In the window that will open, on the **Source** tab, click the **Add** link.
6. Select an FTP or HTTP site, or enter its IP address, symbolic name or URL in the **Select update source** window that will open.

USING A PROXY SERVER

If you are using a proxy server to connect to the Internet, you should edit its settings.

To configure the proxy server, please do the following:

1. Openthe main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.

3. Select the **My Update Center** section in the left part of the window.
4. Click the **Settings** button in the **Update source** section.
5. In the window that will open, on the **Source** tab, click the **Proxy server** button.
6. Edit the proxy server settings in the **Proxy server settings** window that will open.

REGIONAL SETTINGS

If you use Kaspersky Lab update servers as update source, you can select the optimal server location when downloading updates. Kaspersky Lab servers are located in several countries. Choosing the Kaspersky Lab update server closest to you will let you save time and download updates faster.

To choose the closest server:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. Select the **My Update Center** section in the left part of the window.
4. Click the **Settings** button in the **Update source** section.
5. In the window that will open, on the **Source** tab, in the **Regional settings** section, check the **Select from the list** box, and then select the country nearest to your current location from the dropdown list.

   If you select the **Detect automatically** option, the information on your location will be copied from your operating system's registry when updating.

ACTIONS TO BE PERFORMED AFTER THE UPDATE

Computer Protection also allows you to specify actions which will be performed automatically after the update. The following possible actions are available:

- **Rescan quarantine**. The quarantine area contains objects that have been flagged by the application as suspicious or possibly infected. Possibly, after database update the product will be able to recognize the threat unambiguously and neutralize it. Due to this fact the application scans quarantine objects after each update. For this reason the application scans quarantined objects after each update. Scanning may change their status. Some objects can then be restored to the previous locations, and you will be able to continue working with them.
- **Copy updates to folder**. If computers are linked in a home LAN, updates do not need to be downloaded and installed on each computer individually. You can use the update distribution service to save network bandwidth, as the service ensures that the updates are downloaded only once.

In order to scan quarantined files after the update:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. Select the **My Update Center** section in the left part of the window.
4. Check the **Rescan quarantine after update** box in the **Additional** section.

UPDATE: FROM A LOCAL FOLDER

The procedure of retrieving updates from a local folder is arranged as follows:

1. One of the computers on the network retrieves the Computer Protection update package from Kaspersky Lab's updates servers, or from a mirror server hosting a current set of updates. The updates retrieved are placed in a shared folder.

2. Other computers on the network access the shared folder to retrieve Computer Protection updates.

To enable updates distribution mode:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. Select the **My Update Center** section in the left part of the window.

4. Check the **Copy updates to folder** box in the **Additional** section and specify the path to a public folder into which all downloaded updates will be copied in the field below. You can also select the path in the dialog displayed after clicking the **Browse** button.

If you wish updates to be performed from the selected public access folder, perform these actions on all computers in the network:

1. Open the main application window and click the **My Computer Protection**.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. Select the **My Update Center** section in the left part of the window.

4. Click the **Settings** button in the **Update source** section.

5. In the window that will open, on the **Source** tab, click the **Add** link.

6. In the **Select update source** window that will open, select a folder or enter the full path to it in the **Source** field.

7. Uncheck the **Kaspersky Lab's update servers** box on the **Source** tab.

CHANGING THE UPDATE TASK RUN MODE

You should select the startup mode for the Computer Protection update task when the Computer Protection Configuration Wizard is active (see section "Step 4. Configuring application update" on page 41). If you wish to modify the selected update startup mode, you can reconfigure it.

The update task can be launched using one of the following modes:

- **Automatically**. Computer Protection checks the update source for updates at specified intervals. Scanning frequency can be increased during anti-virus outbreaks and decreased when there are none. Having discovered new updates, the program downloads and installs them on the computer.

- **By schedule** (time interval changes depending on settings). Updates will run automatically according to the schedule created.

- **Manually**. If you select this option, you will run Computer Protection updates on your own.

To configure the update task launch schedule:

1. Open the main application window and click the **My Computer Protection** button.

2. In the window that will open, click the **Settings** link in the top part of the window.

3. Select the **My Update Center** section in the left part of the window.

4. Click the **Settings** button in the **Run mode** section.

5. In the window that will open, on the **Run mode** tab, select the update task startup mode in the **Schedule** section. If the **By schedule** option is selected, create the schedule.

   If an update was skipped for any reason (for example, the computer was not on at that time), you can configure the task to start automatically as soon as it becomes possible. To do so, check the **Run skipped tasks** box in the bottom part of the window. This checkbox is available for all schedule options, except **Hours**, **Minutes** and **After application startup**.

RUNNING UPDATES UNDER A DIFFERENT USER'S ACCOUNT

By default, the update procedure is run under your system account. However, Computer Protection can update from a source for which you have no access rights (for example, from a network folder containing updates) or authorized proxy user credentials. You can run Computer Protection update under the account of a user who has the necessary rights.

To start the update under a different user's account:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. Select the **My Update Center** section in the left part of the window.
4. Click the **Settings** button in the **Run mode** section.
5. In the window that will open, on the **Run mode** tab, in the **User account** block, check the **Run task as** box. Specify the user name and password.

CONFIGURING COMPUTER PROTECTION SETTINGS

The application settings window is used for quick access to the main Computer Protection settings.

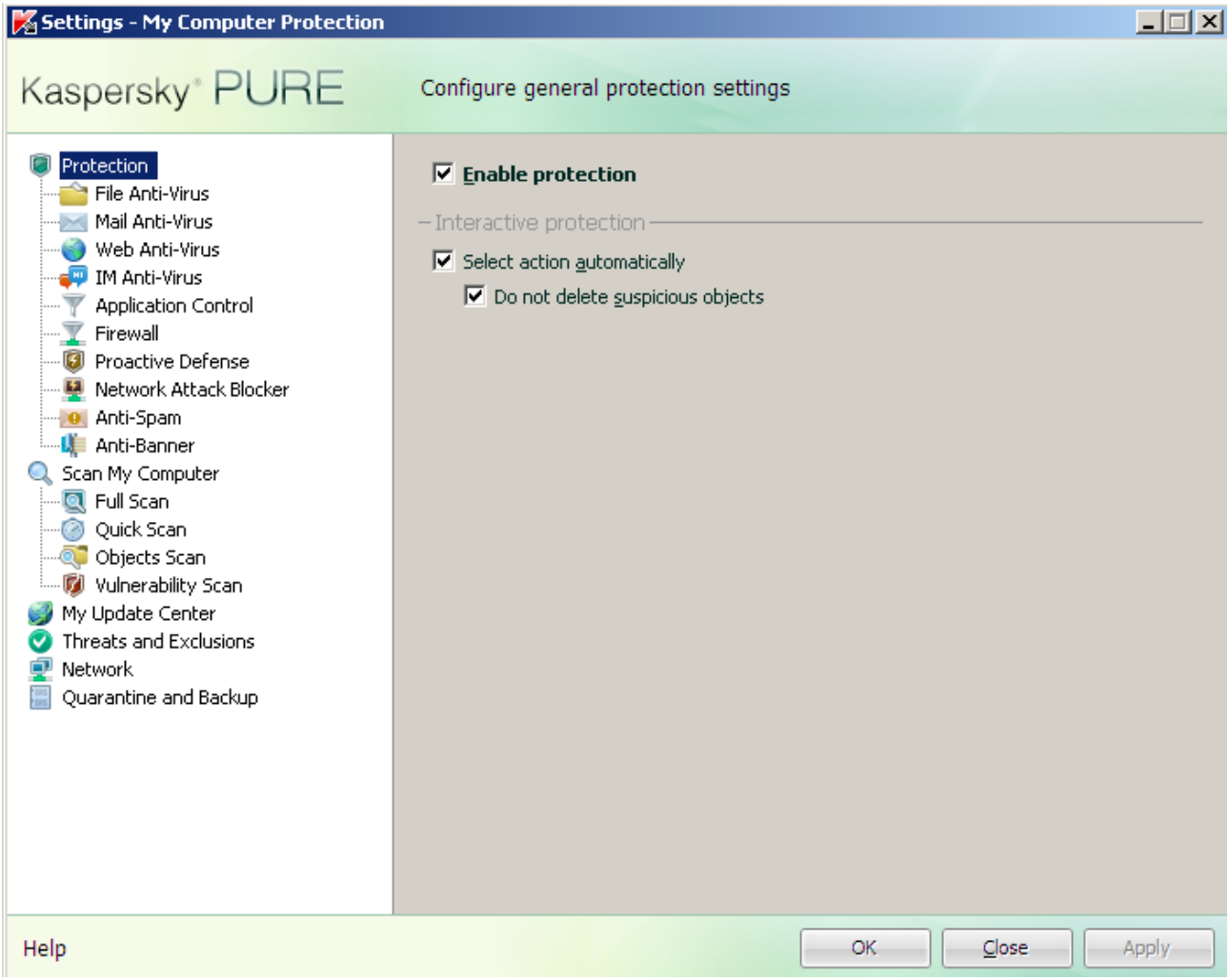


Figure 14. Application settings window

The application settings window consists of two parts:

- the left part of the window provides access to Computer Protection components, virus scan tasks, update tasks, etc.;
- the right part of the window contains a list of settings for the component, task, etc., selected in the left part of the window.

You can open this window:

- From the main application window (see section "My Computer Protection" on page 53). To do so, click the **Settings** link in the top part of the main window.

- from the context menu (see section "Context menu" on page 50). To do so, select the **Settings** item from the application context menu.

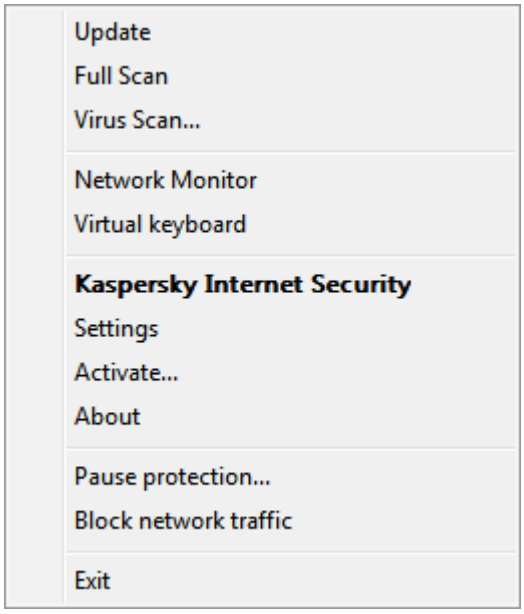


Figure 15. Context menu

IN THIS SECTION:

PROTECTION

In the **Protection** window you can use the following additional functions of Computer Protection:

- Enabling / disabling the protection provided by Computer Protection (see page 156).
- Using interactive protection mode (see page 156).

ENABLING / DISABLING COMPUTER PROTECTION

By default, Computer Protection is launched when the operating system loads, and protects your computer until it is switched off. All protection components are running.

You can completely or partially disable the protection provided by Computer Protection.

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

When the protection is disabled, all its components become inactive. This is indicated by the following signs:

- inactive (grey) icon of My Computer Protection (see section "Notification area icon" on page 50) in the taskbar notification area;
- red color of the security indicator.

In this case protection is being discussed in the context of the protection components. Disabling or pausing protection components does not affect the execution of virus scan tasks and Computer Protection updates.

To disable protection completely:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open select the **Protection** section.
4. Uncheck the **Enable protection** box.

USING INTERACTIVE PROTECTION MODE

Computer Protection uses two modes to interact with the user:

- *Interactive protection mode*. Computer Protection notifies the user about all hazardous and suspicious events occurring in the system. In this mode the user independently decides whether to allow or block actions.
- *Automatic protection mode*. Computer Protection will automatically apply actions recommended by Kaspersky Lab specialists in response to dangerous events.

To use the automatic protection mode:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open select the **Protection** section.

4. In the **Interactive protection** section, check the **Select action automatically** box. If you do not want Computer Protection to delete suspicious objects when running in automatic mode, check the **Do not delete suspicious objects** box.

FILE ANTI-VIRUS

The File Anti-Virus component's settings are grouped in the window (see section "Computer file system protection" on page 59). You can perform the following actions by editing the settings:

- disable File Anti-Virus;
- change security level (see page 61);
- change action to be performed on detected objects (see page 61);
- create a protection scope (see page 62);
- optimize the scan (see page 63);
- configure the scan of compound files (see page 64);
- change the scan mode (see page 65);
- use the heuristic analysis (see page 63);
- pause the component (see page 66);
- select a scan technology (see page 65);
- restore the default protection settings (see page 67) if they have been edited.

To disable File Anti-Virus, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **File Anti-Virus** component.
4. Uncheck the **Enable File Anti-Virus** box in the right part of the window.

To proceed to the File Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **File Anti-Virus** component.
4. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Settings** button in order to switch to the other File Anti- Virus settings.

MAIL ANTI-VIRUS

The Mail Anti-Virus component settings are grouped in the window (see section "Mail protection" on page 69). You can perform the following actions by editing the settings:

- disable Mail Anti-Virus;

- change security level (see page 70);
- change action to be performed on detected objects (see page 71);
- create a protection scope (see page 71);
- use the heuristic analysis (see page 73);
- configure the scan of compound files (see page 74);
- configure filtering the objects attached to the email message (see page 74);
- restore the default email protection settings (see page 74).

To disable Mail Anti-Virus, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Mail Anti-Virus** component.
4. Uncheck the **Enable Mail Anti-Virus** box in the right part of the window.

To proceed to the Mail Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Mail Anti-Virus** component.
4. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Settings** button in order to switch to the other Mail Anti-Virus settings.

WEB ANTI-VIRUS

The Web Anti-Virus component settings are grouped in the window (see section "Web traffic protection" on page 76). You can perform the following actions by editing the settings:

- disable Web Anti-Virus;
- change security level (see page 78);
- change action to be performed on detected objects (see page 78);
- create a protection scope (see page 78);
- change scan methods (see page 79);
- use the Kaspersky URL Advisor (see page 80);
- optimize the scan (see page 81);
- use the heuristic analysis (see page 81);
- restore the default Web Anti-Virus settings (see page 82).

To disable Web Anti-Virus, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Web Anti-Virus** component.
4. Uncheck the **Enable Web Anti-Virus** box in the right part of the window.

To proceed to the Web Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Web Anti-Virus** component.
4. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Settings** button in order to switch to the other Web Anti-Virus settings.

IM ANTI-VIRUS

The IM Anti-Virus component settings are grouped in the window (see section "Protecting instant messengers traffic" on page 83). You can perform the following actions by editing the settings:

- disable IM Anti-Virus;
- create a protection scope (see page 84);
- change the scan method (see page 84);
- use the heuristic analysis (see page 85).

To disable IM Anti-Virus, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **IM Anti-Virus** component.
4. Uncheck the **Enable IM Anti-Virus** box in the right part of the window.

To proceed to the IM Anti-Virus settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **IM Anti-Virus** component.
4. In the right part of the window, make the required changes of the component settings.

APPLICATION CONTROL

The Application Control settings are grouped in this window (see page 86). You can perform the following actions by editing the settings:

- disable Application Control;
- create a protection scope (see page 89);
- manage placing applications into groups (see page 91);
- change the time for determining the application status (see page 92);
- change the rule for application (see page 92);
- change the rule for a group of applications (see page 93);
- create a network rule for the application (see page 93);
- specify exclusions (see page 94);
- manage deleting rules for applications (see page 94).

To disable Application Control, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. In the right part of the window, uncheck the **Enable Application Control** box.

To edit Application Control settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Application Control** component.
4. In the right part of the window, make the required changes of the component settings.

FIREWALL

The Firewall component settings are grouped in this window (see page 100). You can perform the following actions by editing the settings:

- disable Firewall;
- change the network's status (see page 100);
- extend the range of network addresses (see page 101);
- select the mode of notification about changes in network (see page 101);
- specify the advanced component settings (see page 102);
- specify the Firewall rules (see page 102):
  - create a packet rule (see page 103);
  - create a rule for the application (see page 103);
  - use the Rule Creation Wizard (see page 104);

- select the action to be performed by the rule (see page 105);
- edit the network service settings (see page 105);
- select the range of addresses (see page 106);
- change the rule's priority.

To disable the Firewall, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Firewall** component.
4. Uncheck the **Enable Firewall** box in the right part of the window.

To proceed to editing the Firewall settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Firewall** component.
4. In the right part of the window, click the **Settings** button, and make the required changes of the component settings in the window that will open.

PROACTIVE DEFENSE

The Proactive Defense component settings are grouped in this window (see page 107). You can perform the following actions by editing the settings:

- disable Proactive Defense;
- manage the list of dangerous activity (see page 107);
- change the application's reaction to dangerous activity in the system (see page 108);
- create a group of trusted applications (see page 109);
- monitor system user accounts (see page 109).

To disable Proactive Defense, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Proactive Defense** component.
4. Uncheck the **Enable Proactive Defense** box in the right part of the window.

To proceed to editing the Proactive Defense settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.

3. In the window that will open, in the **Protection** section, select the **Proactive Defense** component.
4. In the right part of the window, make the required changes of the component settings.

NETWORK ATTACK BLOCKER

This window groups the settings of the Network Attack Blocker component (see page 110). You can perform the following actions by editing the settings:

- disable Network Attack Blocker;
- add an attacking computer to blocked list (see page 110).

To disable Network Attack Blocker, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Network Attack Blocker** component.
4. In the right part of the window, uncheck the **Enable Network Attack Blocker** box.

To switch to editing the Network Attack Blocker settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Network Attack Blocker** component.
4. In the right part of the window, make the required changes of the component settings.

ANTI-SPAM

The Anti-Spam component settings are grouped in this window (see page 113). You can perform the following actions by editing the settings:

- disable Anti-Spam;
- train Anti-Spam (see page 115):
  - using the Training Wizard (see page 116);
  - with outgoing messages (see page 117);
  - using email client (see page 117);
  - using the reports (see page 118);
- change security level (see page 119);
- change the scan method (see page 119);
- create a list of:
  - trusted URLs (see page 120);
  - blocked senders (see page 120);

- blocked phrases (see page 121);
- obscene phrases (see page 122);
- allowed senders (see page 122);
- allowed phrases (see page 123);

- import the list of allowed senders (see page 124);
- determine spam and potential spam ratings (see page 124);
- select the spam recognition algorithm (see page 125);
- use additional spam filtering features (see page 125);
- add a label to the message's subject (see page 126);
- use Mail Dispatcher (see page 126);
- exclude from scan Microsoft Exchange Server messages (see page 127);
- configure spam processing:
  - in Microsoft Office Outlook (see page 127);
  - in Microsoft Outlook Express (Windows Mail) (see page 129);
  - in The Bat! (see page 129);
  - in Thunderbird (see page 130);
- restore the default Anti-Spam settings (see page 130).

To disable Anti-Spam, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Anti-Spam** component.
4. Uncheck the **Enable Anti-Spam** box in the right part of the window.

To proceed to editing the Anti-Spam settings, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Anti-Spam** component.
4. In the right part of the window, click the **Settings** button, and make the required changes of the component settings in the window that will open.

ANTI-BANNER

The Anti-Banner component settings are grouped in this window (see page 131). You can perform the following actions by editing the settings:

- disable Anti-Banner;
- use the heuristic analysis (see page 131);
- specify the advanced component settings (see page 132);
- create the list of allowed addresses (see page 132);
- create the list of blocked addresses (see page 132);
- export / import banner lists (see page 133).

To disable Anti-Banner, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Anti-Banner** component.
4. Uncheck the **Enable Anti-Banner** box in the right part of the window.

To proceed to editing the Anti-Banner settings, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, in the **Protection** section, select the **Anti-Banner** component.
4. In the right part of the window, make the required changes of the component settings.

SCAN MY COMPUTER

Selection of the method to be used to scan objects on your computer is determined by the set of properties assigned for each task.

Kaspersky Lab distinguishes virus scan tasks and vulnerability scan tasks. Virus scan tasks include the following:

- **Object Scan**. Scan of objects selected by the user. You can scan any object in the computer's file system.
- **Full Scan**. A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded on startup, system backup, email databases, hard drives, removable storage media and network drives.
- **Quick Scan**. Virus scan of operating system startup objects.

You can perform the following actions in the settings window for each virus scan task:

- select the security level with the relevant settings defining task behavior at runtime;
- select the action that the application will apply when it detects an infected / potentially infected object;
- create a schedule to run tasks automatically;
- create a list of objects to be scanned (for quick scan and full scan tasks);
- specify the file types to be scanned for viruses;
- specify the scan settings for compound files;

- select the scan methods and scan technologies.

In the **Scan My Computer** section, you can specify the settings for the automatic scan of removable drives when connecting them to your computer, and create shortcuts for the quick start of virus scan and vulnerability scan tasks.

In the settings window, you can perform the following actions for a vulnerability scan task:

- create a schedule to run tasks automatically;
- create a list of objects to be scanned.

To edit task settings:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, select the required task in the **Scan My Computer** (**Full Scan**, **Quick Scan**, **Object Scan**, **Vulnerability Scan**) section.
4. Configure the settings in the right part of the window.

UPDATE

The update of Computer Protection is performed according to the set of parameters.

You can perform the following actions from the update task configuration window:

- change the address of the resource from which application updates will be distributed and installed;
- specify the type of a mode, according to which the application update process will be started;
- set the run schedule for a task;
- specify the account under which the update will be started;
- select actions which should be performed after application update.

To proceed to update configuration:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. Select the **My Update Center** section in the left part of the window.
4. Select the required run mode in the right part of the window and select an update source. Configure other task settings in the **Additional** section.

SETTINGS

In the **Settings** window, you can use the following additional functions of Computer Protection:

- Select detectable threat categories (see page 166).
- Create the trusted zone for the application (see page 166).
- Create exclusion rules (see page 167).

- Create a list of monitored ports (see page 169);
- Enable / disable the encrypted connections scan mode (using the SSL protocol) (see page 170);
- Configure Quarantine and Backup (see page 172).

THREATS AND EXCLUSIONS

In the **Threats and Exclusions** section of the Computer Protection settings window, you can perform the following actions:

- select detectable threat categories (see section "Selecting the detectable threat categories" on page 166);
- create the trusted zone for the application.

Trusted zone is the user-created list of objects which should not be controlled by the application. In other words, it is a set of exclusions from the scope of Computer Protection.

Trusted zone is created based on the list of trusted applications (see section "Selecting trusted applications" on page 166) and exclusion rules (see section "Exclusion rules" on page 167).

The user creates a trusted zone based on the features of the objects he or she works with, and on the applications installed on the computer. You might need to create such an exclusion list if, for example, the application blocks access to an object or program which you are sure is absolutely safe.

SEE ALSO:

SELECTING DETECTABLE THREAT CATEGORIES

Computer Protection protects you against various types of malicious programs. Regardless of the settings selected, the application will always scan and disinfect viruses, Trojans and hacker utilities. These programs can do significant harm to your computer. To provide more security to your computer, you can enlarge the list of threats to be detected, by enabling the control of various potentially dangerous programs.

To select the detectable threat categories, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, select the **Threats and exclusions** section. Click the **Settings** button in the **Threats** section.
4. In the **Threats** window that will open select the categories of threats you wish to protect your computer against.

SELECTING TRUSTED APPLICATIONS

You can create a list of trusted applications which will allow not to control the file and network activity (including the suspicious one) from their part, as well as attempts to access the system registry.

For example, you may feel that objects used by Microsoft Windows Notepad are safe and do not need to be scanned. In other words, you do trust this application. To exclude from scan the objects used by this process, add the Notepad application to the list of trusted applications. At the same time, the executable file and the trusted application's process will be scanned for viruses as they were before. To completely exclude an application from the scan, you should use exclusion rules.

Besides, some actions classified as dangerous may be stated as normal by a number of applications. For example, applications that automatically toggle keyboard layouts, such as Punto Switcher, regularly intercept text being entered on your keyboard. To take into account the specifics of such applications and disable the monitoring of their activity, you are advised to add them to the list of trusted applications.

Excluding trusted applications from the scan allows solving probable problems of the application's compatibility with other programs (e.g. the problem of double scanning of network traffic of a third-party computer by Computer Protection and by another anti-virus application), as well as increase the computer's performance rate which is critical when using server applications.

By default, Computer Protection scans objects being opened, run, or saved by any program process, and monitors the activity of all applications and the network traffic they create.

To add an application to the trusted list, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, select the **Threats and exclusions** section.
4. In the **Exclusions** section, click the **Settings** button.
5. In the window that will open, on the **Trusted applications** tab, click the **Add** link.
6. In the menu that will open, select an application. Once you select the **Browse** item, a window will open in which you should specify the path to an executable file. Once you select the **Applications** item, the list of applications currently running will open.
7. In the **Exclusions for applications** window that will open, specify the rule settings for the application.

Note that if the **Do not scan network traffic** box is checked, the traffic of the application specified will not be scanned for viruses and spam only. However, this does not affect the traffic scan by the Firewall component. Firewall settings govern the analysis of network activity for that application.

You can change or delete the trusted application from the list using the corresponding links in the bottom part of the tab. To remove an application from the list without its actual deletion, uncheck the box next to its name.

EXCLUSION RULES

Potentially dangerous software does not have any malicious functions but can be used as an auxiliary component for a malicious code, since it contains holes and errors. This category includes, for example, remote administration programs, IRC clients, FTP servers, various utilities for halting or concealing processes, keyloggers, password crackers, autodialers, etc. These programs are not classified as viruses (not-a-virus). They can be subdivided into different types, such as Adware, Joke, Riskware, etc. (for more details on potentially dangerous programs detected by the application see the Virus Encyclopedia at www.viruslist.com). After the scan, such programs may be blocked. Since several of them are widely used by users, you have the option of excluding them from the scan.

For example, you may frequently use the Remote Administrator program. This is a remote access program which allows you to work on a remote computer. Computer Protection views the activity of this program as potentially dangerous, and may block it. If you do not wish the application to be blocked, you should create an exclusion rule for the application which is detected as *not-a-virus:RemoteAdmin.Win32.RAdmin.22* according to the Virus Encyclopedia.

Exclusion rules are sets of conditions that Computer Protection uses to verify if it can skip an object during the scan.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects according to the Virus Encyclopedia's threat type classification.

Threat type is the status Computer Protection assigns to an object during the scan. A status is assigned based on the classification of malicious and potentially dangerous programs listed in the Kaspersky Lab's Virus Encyclopedia.

Adding an exclusion creates a rule that can be used by several application components (such as File Anti-Virus (see section "Computer file system protection" on page 59), Mail Anti-Virus (see section "Mail protection" on page 69), Web Anti-Virus (see section "Web traffic protection" on page 76)), and by virus scan tasks.

To create an exclusion rule, please do the following:

1. Open the main application window and click the **My Computer Protection** button.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, select the **Threats and exclusions** section.
4. In the **Exclusions** section, click the **Settings** button.
5. In the window that will open, on the **Exclusion rules** tab, click the **Add** link.
6. In the **Exclusion rule** window that will open, edit the exclusion rule settings.

SEE ALSO:

ALLOWED FILE EXCLUSION MASKS

Let's look at some examples of permitted masks that you can use when create file exclusion lists. They are as follows:

1. Masks without file paths:
   - ***.exe** – all files with the *exe* extension;
   - ***.ex?** – all files with the *ex?* extension, where **?** can represent any single character;
   - **test** – all files with the name *test.*
2. Masks with absolute file paths:
   - **C:\dir*.*** or **C:\dir*** or **C:\dir** – all files in the *C:\dir* folder;
   - **C:\dir*.exe** – all files with the exe extension in the *C:\dir* folder;
   - **C:\dir*.ex?** – all files with the *ex?* extension; in folder *C:\dir*, where **?** can represent any single character;
   - **C:\dir\test** – only the *C:\dir\test* file.

     If you wish to exclude file scan in all nested folders of the specified folder, check the **Include subfolders** box when creating a mask.
3. File path masks:
   - **dir*.***, or **dir***, or **dir** – all files in all *dir* folders;
   - **dir\test** – all *test* files in *dir* folders;
   - **dir*.exe** – all files with the *exe* extension in all *dir* folders;
   - **dir*.ex?** – all files with the *ex?* extension; in all *dir* folders, where **?** can represent any single character.

If you wish to exclude file scan in all nested folders of the specified folder, check the **Include subfolders** box when creating a mask.

. and * exclusion masks can only be used if you specify the classification type of the threat according to the Virus Encyclopedia. In this case, the specified threat will not be detected in any object. Using those masks without specifying the classification type essentially disables monitoring. When setting an exclusion, it is not recommended selecting a path related to a network disk created based on a file system folder using the subst command, as well as to a disk, which mirrors a network folder. The case is that different resources may be given the same disk name for different users, which will inevitably lead to an incorrect triggering of exclusion rules.

ALLOWED THREAT TYPE MASKS

When adding masks to exclude certain threats based upon their Virus Encyclopedia classification, you can specify the following settings:

- The full name of the threat as given in the Virus Encyclopedia at *www.viruslist.com* (e.g. *not-a-virus:RiskWare.RemoteAdmin.RA.311* or *Flooder.Win32.Fuxx*).
- The threat name by mask, e.g.:
  - **not-a-virus*** – exclude legal but potentially dangerous programs from the scan, as well as joke programs;
  - ***Riskware.*** – exclude riskware from the scan;
  - ***RemoteAdmin.*** – exclude all remote administration programs from the scan.

NETWORK

In the **Network** section of the application settings window, you can select the ports monitored by Computer Protection, and configure the scan of encrypted connections:

- create a list of monitored ports (see page 169);
- Enable / disable the encrypted connections scan mode (using the SSL protocol) (see page 170);

SEE ALSO:

CREATING A LIST OF MONITORED PORTS

Protection components, such as Mail Anti-Virus (see section "Mail protection" on page 69), Web Anti-Virus (see section "Web traffic protection" on page 76), and Anti-Spam (see page 113), monitor data streams transmitted via certain protocols and passing via certain opened ports on your computer. Thus, for example, Mail Anti-Virus analyzes information transferred via the SMTP protocol, and Web Anti-Virus analyzes HTTP packets.

You can select one of two port monitoring modes:

- **Monitor all network ports**;
- **Monitor selected ports only**. A list of ports that are used for transmitted email and HTTP traffic is included in the application package.

- *In order to add a port to the list of monitored ports:*

  1. Open the main application window and click the **My Computer Protection** button.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, select the **Network** section.
  4. In the **Monitored ports** section click the **Select** button.
  5. In the **Network ports** window that will open, click the **Add** link.
  6. In the **Network port** window that will open, specify the required data.

- *In order to exclude a port from the list of monitored ports:*

  1. Open the main application window and click the **My Computer Protection** button.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, select the **Network** section.
  4. In the **Monitored ports** section click the **Select** button.
  5. In the **Network ports** window that will open, uncheck the box next to the port's description.

- *To create the list of applications for which you wish to monitor all the ports, please do the following:*

  1. Open the main application window and click the **My Computer Protection**.
  2. In the window that will open, click the **Settings** link in the top part of the window.
  3. In the window that will open, select the **Network** section.
  4. In the **Monitored ports** section click the **Select** button.
  5. In the **Network ports** window that will open, check the **Monitor all ports for specified applications** box and click the **Add** link in the section below.
  6. In the menu that will open, select an application. Once you select the **Browse** item, a window will open in which you should specify the path to an executable file. Once you select the **Applications** item, the list of applications currently running will open.
  7. In the **Application** window that will open, specify the description for the application selected.

SCANNING ENCRYPTED CONNECTIONS

Connecting using the Secure Sockets Layer (SSL) protocol protects data exchange channel on the Internet. The SSL protocol allows to identify the parties exchanging data using electronic certificates, encode the data being transferred, and ensure their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus programs do not scan SSL traffic.

Computer Protection verifies secure connections sing Kaspersky Lab certificate. This certificate will always be used to check whether the connection is secure.

Further traffic scans via the SSL protocol will be performed using the installed Kaspersky Lab's certificate. If an invalid certificate is detected when connecting to the server (for example, if the certificate is replaced by an intruder), a notification will pop up containing a suggestion to either accept or reject the certificate, or view information about the certificate. If the application works in automatic mode, the connection using an invalid certificate will be terminated without any notification.

To enable encrypted connections scan, please do the following:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, select the **Network** section.
4. In the window that will open, check the **Scan encrypted connections** box and click the **Install certificate** button.
5. In the window that will open, click the **Install Certificate** button. This will start a wizard with instructions to follow for a successful installation of the certificate.

The automatic installation of the certificate will only be available in Microsoft Internet Explorer. To scan encrypted connections in Mozilla Firefox or Opera, you should install the Kaspersky Lab's certificate manually.

SCANNING ENCRYPTED CONNECTIONS IN MOZILLA FIREFOX

Mozilla Firefox browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Firefox, you should install the Kaspersky Lab's certificate manually.

To install the Kaspersky Lab's certificate please do the following:

1. In the browser's menu, select the **Tools** → **Settings** item.
2. In the window that will open, select the **Additional** section.
3. In the **Certificates** section, select the **Security** tab and click the **Viewing certificates** button.
4. In the window that will open, select the **Certification Centers** tab and click the **Restore** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
   %AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.
6. In the window that will open, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

To install the Kaspersky Lab's certificate for Mozilla Firefox version 3.x, please do the following:

1. In the browser's menu, select the **Tools** → **Settings** item.
2. In the window that will open, select the **Additional** section.
3. On the **Encryption** tab, click the **Viewing certificates** button.
4. In the window that will open, select the **Certification Centers** tab and click the **Import** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
   %AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.
6. In the window that will open, check the boxes to select the actions that should be scanned with the certificate installed. To view information about the certificate, click the **View** button.

If your computer runs under Microsoft Windows Vista, the path to the Kaspersky Lab's certificate file will be as follows: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SCANNING ENCRYPTED CONNECTIONS IN OPERA

Opera browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Opera, you should install the Kaspersky Lab's certificate manually.

To install the Kaspersky Lab's certificate please do the following:

1. In the browser's menu, select the **Tools** → **Settings** item.
2. In the window that will open, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that will open, select the **Vendors** tab and click the **Import** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.
6. In the window that will open, click the **Install** button. Kaspersky Lab's certificate will be installed. To view information about the certificate, and to select actions for which the certificate will be used, select the certificate in the list and click the **View** button.

To install the Kaspersky Lab's certificate for Opera version 9.x, please do the following:

1. In the browser's menu, select the **Tools** → **Settings** item.
2. In the window that will open, select the **Additional** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that will open, select the **Certification Centers** tab and click the **Import** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows:
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.
6. In the window that will open, click the **Install** button. Kaspersky Lab's certificate will be installed.

If your computer runs under Microsoft Windows Vista, the path to the Kaspersky Lab's certificate file will be as follows: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

QUARANTINE AND BACKUP

The section contains the settings that control the operation with Computer Protection data files.

Application data files are objects that have been moved to Quarantine and Backup by Computer Protection. In this section, you can configure Quarantine and Backup (see page 174).

SEE ALSO:

QUARANTINE FOR POTENTIALLY INFECTED OBJECTS

Quarantine is a special repository that stores the objects possibly infected with viruses.

Potentially infected objects are objects that are suspected of being infected with viruses or their modifications.

A potentially infected object can be detected and quarantined by File Anti-Virus, Mail Anti-Virus, Proactive Defense or in the course of a virus scan.

Objects are placed to quarantine as a result of File Anti-Virus and Mail Anti-Virus operation, as well as in the course of a virus scan, if:

- *The code of the object being analyzed resembles a known threat but is partially modified*.

  Computer Protection databases contain information on the threats investigated to date by Kaspersky Lab's specialists. If a malicious program is modified and these changes have not been entered into the databases yet, Computer Protection classifies the object infected with the modified malicious program as a potentially infected object, and indicates without fail what threat this infection resembles.

- *The code of the object detected is reminiscent in structure of a malicious program; however, nothing similar is recorded in the application databases*.

  It is quite possible that this is a new type of threat, so Computer Protection classifies that object as a potentially infected object.

Files are identified as potentially infected with a virus by the *heuristic code analyzer*. This mechanism is fairly effective and very rarely leads to false positives.

As for Proactive Defense, the component places an object to quarantine if, as a result of behavior analysis, the sequence of object's actions arouses suspicion.

When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk or email, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

It is possible that after database update, Computer Protection will be able to identify the threat unambiguously, and will neutralize it. Due to this fact the application scans quarantine objects after each update.

BACKUP COPIES OF DANGEROUS OBJECTS

Sometimes the integrity of objects cannot be maintained during disinfection. If the disinfected file contained important information, and after disinfection it became inaccessible in part or in full, you can attempt to restore the original object from its backup copy.

Backup copy is a copy of the original dangerous object that is created when first disinfecting or deleting the object, and it is saved in backup.

Backup is a special repository that contains backup copies of dangerous objects after processing or deletion. The main function of a backup storage is the ability to restore the original object at any time. Files in backup are saved in a special format and are not dangerous.

ACTIONS WITH QUARANTINED OBJECTS

You can perform the following actions on the quarantined objects:

- quarantine the files that you suspect of being infected;
- scan and disinfect all potentially infected objects in the quarantine using the current Computer Protection databases;
- restore files to the folders from which they were moved to quarantine, or to the folders selected by the user;
- delete any quarantined object or a group of selected objects;
- send quarantined object to Kaspersky Lab for analysis.

To perform some actions on the quarantined objects:

1. Open the main application window and click the **Quarantine**.
2. Perform the required actions in the window that will open on the **Detected threats** tab.

STORING THE QUARANTINE AND BACKUP OBJECTS

You can edit the following settings for the quarantine and the backup:

- Determine the maximum storage time for quarantined objects and for copies of objects in the backup (the **Store objects no longer than** box). By default, the objects storage time is 30 days; once it expires, the objects will be deleted. You can change the maximum storage term or remove this restriction altogether.
- Specify the maximum size of data storage area (the **Maximum size** box). By default, the maximum size is 100 MB. You can cancel the report size limit or set another value for it.

To configure the quarantine and backup settings:

1. Open the main application window and click the **My Computer Protection**.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the window that will open, select the **Reports and Storages** section.
4. In the **Quarantine and Backup** section, check the required boxes and enter the maximum size of data storage area, if necessary.

REPORTS

The operation of each component of Computer Protection and the performance of each virus scan and update are recorded in a report.

While working with reports you can perform the following actions:

- select the component or task (see page 175) for which you wish to view the event report;
- manage data grouping (see page 176) and displaying data on screen (see page 177);
- create a schedule (see page 176) according to which Computer Protection will remind you about report readiness;
- select the type of events (see page 176) for which you wish to create a report;
- select the mode of displaying (see page 178) statistics on the screen;
- save report as a file (see page 179);
- specify complex filtering conditions (see page 179);
- configure the search for events (see page 180) which occurred in the system and were processed by the application.

IN THIS SECTION:

SELECTING A COMPONENT OR A TASK TO CREATE A REPORT

You can obtain information about events which occurred during the operation of each of Computer Protection's components, or during the execution of tasks (for example, File Anti-Virus, update, etc.).

In order to create a report on a certain component or a task:

1. Open the main application window and click the **Report** link in the top part.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.

3. In the window that will open, select a component or a task, for which a report should be created, in the dropdown list on the left. Once you select the **My Protection** item, report will be created for all protection components.

MANAGING GROUPING OF INFORMATION IN THE REPORT

You can manage how information is grouped in the report, using one of several attributes. The set of attributes differs for each application component and task. The following options exist:

- **Do not group**. All events will be displayed.
- **Group by task**. Data will be grouped by tasks performed by Computer Protection's components.
- **Group by application**. Data will be grouped by applications displaying any activity in the system, and processed by the My Computer Protection module.
- **Group by result**. Data will be grouped based on the results of scan or object processing.

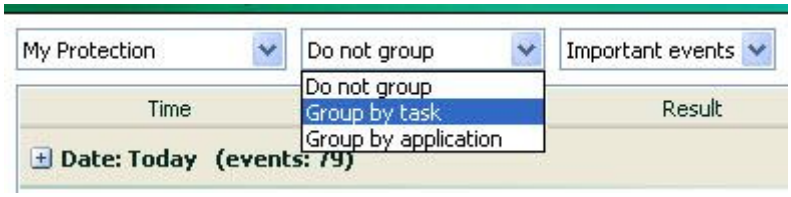


Figure 16. Attributes of grouping of information in the report

To quickly obtain particular information and to decrease the grouping size, a keyword search (see section "Events search" on page 180) criteria is provided. You can also specify a search criteria.

In order to use grouping based on a certain attribute:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. Select the grouping attribute from the drop-down menu in the window that will open.

REPORT READINESS NOTIFICATION

You can create a schedule, according to which Computer Protection will remind you about report readiness.

In order to create a notification schedule:

1. Open themain application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, check the **Notify about the report** box. Click the link with the preset time value.
3. Create the schedule on the **Report: schedule** window that will open.

SELECTING EVENT TYPES

Complete list of all important events occurring in the protection component activity, scan task execution, or application database update, is logged in a report. You can select which type of events will be recorded in the report.

Events can be attributed to the following types:

- *Critical events*. Events of critical importance which indicate problems in Computer Protection's operation, or vulnerabilities in the protection on your computer. They include, for instance, detection of a virus or an operation failure.

- *Important events*. Events that should always be attended to since they reflect important situations in the application's operation, for example, the **terminated** event.

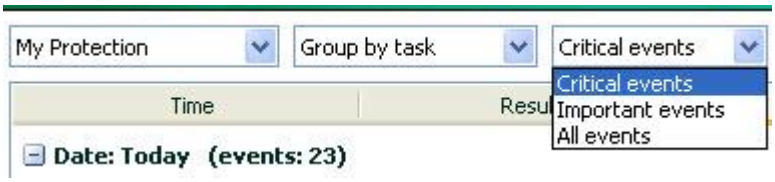


Figure 17. Selecting event type

If the **All events** item is selected, all events will be displayed in the report, but only in case if the corresponding boxes are checked in the **Reports** section of the **Reports and Storages** block of settings. These are boxes which allow to log records of non-critical events as well as file system and registry events, in the report. If these boxes are not checked, a warning icon and the **Disabled** link are displayed near the dropdown event type selection list. Use this link to go to the reports settings window and to check the corresponding boxes.

In order to create a report about a particular event type:

1. Open the main application window and click the **Report** link in the top part of it.

2. In the window that will open, on the **Report** tab, click the **Detailed report** button.

3. Select the event type from the drop-down menu in the window that will open. If report on all events should be created, select the **All events** value.

DISPLAYING DATA ON THE SCREEN

Events included in the report will be displayed as a table. You can create a dataset to filter the information, by specifying a restricting condition. To do this, click the area to the left of the heading of the table column for which you wish to impose a restriction. The dropdown list will display possible values of the restricting conditions, for example, **Yesterday –** for column **Time**, **Email message –** for column **Object** etc. For each column, select the required value. You can choose the most suitable of them; the query will be performed based on the restriction condition you specified. If you wish to view all data, select the **All** item in the list of restrictions.

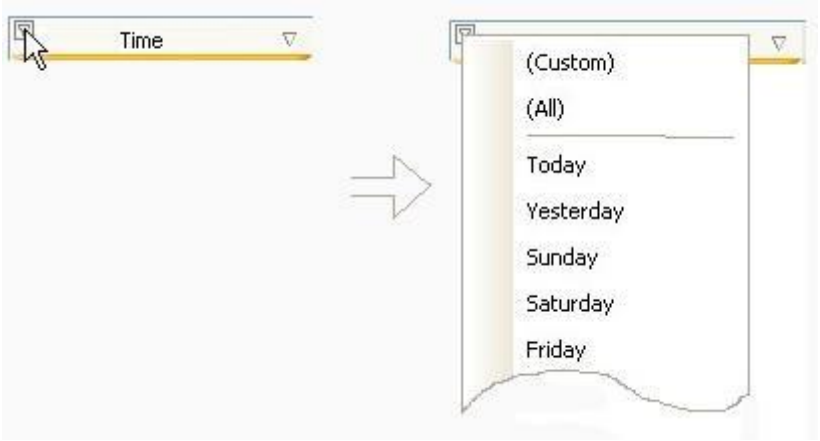


Figure 18. Specifying a restricting condition

You can also specify the settings of a complex search in the form of an interval within which you need to select data about past events. In order to do this, select the **Custom** item in the drop-down list of restrictions. In the window that will open, specify the required time interval (see section "Using complex filtering" on page 179).

For easy and simple report creation, use the context menu to access any attribute that allows grouping and event querying.

Figure 19. Context menu

To specify a limitation:

1. Open the main application window and click the **Report** link in the top part.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, click the area to the left of the heading of the table column for which you wish to impose a restriction. Select a required restriction from the dropdown list. If the **Custom** item is selected, you will be able to specify complex filtering conditions (see section "Using complex filtering" on page 179).

In order to hide / show table columns:

1. Open the main application window and click the **Report** link in the top part of the window.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open, right-click the area to the right of the heading of any table column. To hide any table columns, uncheck boxes next to the corresponding names in the context menu.

EXTENDED DISPLAY MODE FOR STATISTICS

The bottom part of the report window contains statistics on the operation of the selected component or task of Computer Protection. You can view comprehensive statistics in graphic or table presentation (depending on the component or task).

You can switch to viewing the comprehensive statistics using the button in the top part of the window. The statistic is displayed both for the current day, and for the entire period for which the application has been installed on your computer.

To view detailed statistics, please do the following:

1. Open the main application window and click the **Report** link in the top part.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.

3. In the window that will open, select the application component for which you wish to view detailed statistics, and use the button  in the top part of the window.

SAVING A REPORT INTO A FILE

The obtained report can be saved to file.

In order to save the obtained report into a file, perform the following actions:

1. Open the main application window and click the **Report** link in the top part.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.
3. In the window that will open create the required report and click the **Save** button.
4. In the window that will open select a folder into which you wish to save the report file, and enter the file name.

USING COMPLEX FILTERING

The **Custom filter** window (see the figure below) is used to specify complex data filtering conditions. You can use this window to specify data search criteria for any table column. Let us examine the procedure for work with the window using the **Time** column as an example.

A data query using a complex filter is based on the logical conjunction (Logical AND) function and disjunction (Logical OR) function which can be used to control the query.

The query limits (in our case – time) are located in the fields on the right side of the window. To specify the time you can use arrow keys on your keyboard. The dropdown list **Show rows where** is used to pick the condition for events query (for example, **is greater than**, i.e. exceeding the value specified in the field to the right).

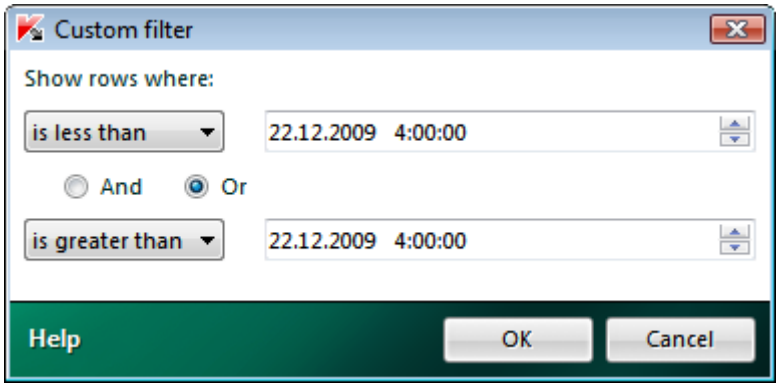


Figure 20. Specifying complex filtering conditions

If you wish your data query to satisfy both specified conditions, select **AND**. If only one of the two conditions is required, select **OR**.

For several types of data the search interval limit is not a numeric or a temporal value, but a word (for example, the query could pick out the **OK** value for the **Result** column). In this case the word specified as the limit will be compared against other word-conditions in alphabetic order.

To specify complex filtering conditions:

1. Open the main application window and click the **Report** link in the top part.
2. In the window that will open, on the **Report** tab, click the **Detailed report** button.

3. In the window that will open, click the area to the left of the table column for which you wish to specify complex filtering conditions. Select the **Custom** item from the dropdown menu. You can also select the **Filter by this field** item from the context menu (see section "Displaying data on the screen" on page 177) displayed after right-clicking the required column of the table.

4. In the **Custom filter** window that will open, specify the required filtration conditions.

EVENTS SEARCH

This window (see fig. below) is designed to search for events that occurred in the system and were processed by Computer Protection.

Provided below is the discussion of the principles used while working with this window.

- The **String** field is used to enter the keyword (for example, explorer). To start the search, click the **Find next** button. The search for the required data may take some time. After the search is complete, events related to the keyword you have entered will be displayed. Clicking the **Mark all** button will select all found entries matching the search keyword.

- The **Column** field is used to select the column of the table on which the keyword search will be performed. This selection allows you to save time required to perform a search (unless, of course, you have not selected the **All** value).

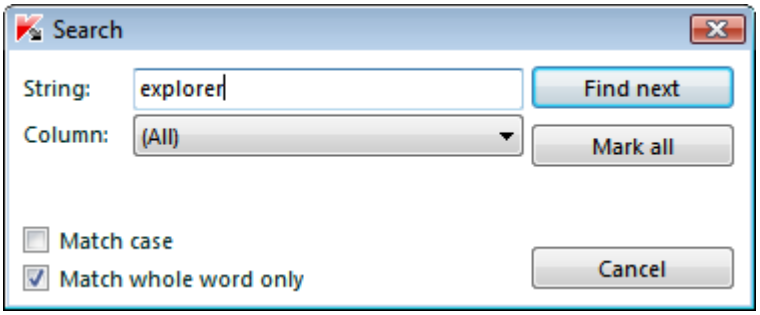


Figure 21. Events search

To make the search case-sensitive, check the **Match case** box. The **Match whole word only** checkbox will restrict the search to finding whole words only.

To use events search:

1. Open the main application window and click the **Report** link in the top part of the window.

2. In the window that will open, on the **Report** tab, click the **Detailed report** button.

3. In the window that will open, right-click the area to the right of the heading of any table column. Select the **Search** item from the context menu.

4. Specify the search criteria in the **Search** window that will open.

BACKUP COPY

During the backup process, backup copies of the chosen files are created in a special storage area.

Backup storage is a specially assigned area of disk space or a data storage media. Storages are used by the backup tasks for storing backup copies of data.

When creating a storage area (see section "Creating a backup storage area" on page 181), the user selects the data medium, specifies the name of the new storage area and the settings for storing backup copies. Also, stored data may be password-protected against unauthorized access. After that, service information about the storage area is recorded onto the data medium.

To carry out data backup, backup tasks are created (see section "Creating a backup task" on page 183). *Backup task* is a user-defined collection of parameters that determines the selection of data subject to backup, storage area for backup copies, and backup conditions. Tasks are restartable (manually or by schedule).

Backup copies of files created within the framework of a single task are stored in *archives*. Archives of backup copies are placed into a storage after having been assigned the name matching that of the task.

Once the necessity of restoring data from backup copies arises, the restoring procedure gets started (see section "Restoring data" on page 185), or the Kaspersky Restore Utility recovery tool is used. Files may be restored from backup copies either into their initial location, or into any available folder.

All events related to backup are recorded into the report (see section "Viewing event report" on page 186).

IN THIS SECTION:

CREATING A BACKUP STORAGE AREA

A backup storage area may be created using the wizard. Backup Storage Creation Wizard may be launched using one of the two following modes:

- from the main module window;
- from the Backup Task Creation Wizard (see section "Creating a backup task" on page 183).

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing links in the top part of the window.

To create a backup storage area, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Storages** section and click the **Create** button.
3. Backup Storage Creation Wizard will be launched. Let us take a closer look at the wizard's steps:
   a. In the left part of the **Drive** window, select the type of data storage medium which will be used as a backup storage.

      To ensure data security, we recommend that you create backup storages on removable disk drives.

   b. In the **Protection** window, set a password to protect data against unauthorized access (if necessary).
   c. In the **Settings** window, set a limit on the number of files' versions which may coexist within the storage, and specify the time interval for storing backup copies (if necessary).
   d. In the **Summary** window, enter the name for the new storage and confirm the storage creation with the settings you have specified.

CONNECTING A STORAGE

If you have created a storage with the Backup module but it is unavailable on the computer you are currently using (for example, after the operating system is reinstalled, or if the storage is copied from another computer), you will need to connect that storage in order to start working with the data.

To connect an existing storage, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Storages** section and click the **Connect** button.
3. Select a storage type and specify the required connection settings in the **Connect storage** window.

   If the settings are specified properly, the storage appears on the list.

CLEARING A STORAGE

If storage volume is not sufficient for your current operations, you can delete obsolete versions and backup copies of files which have been already deleted from the computer.

To clear a storage, please do the following:

1. Open the main application window and click the click the **Backup** button.
2. In the window that will open, select the **Storages** section.
3. Select the storage you wish to clear and click the **Clear** button.
4. In the **Clear storage** window that will open, select the file versions that should be deleted from the storage.

REMOVING A STORAGE

To remove a storage for backup data, you should use Storage Removal Wizard. During the removal, you are asked to determine actions to be performed on the data in the storage, that is to be removed, and on the tasks, that use the storage for backup copying.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

To remove a backup storage, please do the following:

1. Open the main application window and click the click the **Backup** button.
2. In the window that will open, select the **Storages** section.
3. Select the storage you wish to delete and click the **Delete** button.
4. Backup Storage Removal Wizard will be launched. Let us take a closer look at the wizard's steps:
    a. Select an action to perform on the backup copies that are located within the storage to be removed, in the **Content** window.
    b. Select an action to perform with the tasks that use the storage for backup copy, in the **Tasks** window.
    c. Confirm the removal of the storage with selected settings in the **Summary** window.

CREATING A BACKUP TASK

Backup tasks are used for creating backup copies of files.

A backup task may be created using the wizard.

When creating a backup task, the following settings should be defined:

- a set of files for which backup copies will be created;
- a storage in which they will be created;
- conditions of backup process startup.

Backup Task Creation Wizard may be launched using one of the two following modes:

- from the main module window;
- from the Microsoft Windows context menu.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

To create a backup task, please do the following:

1. Open the main application window and click the click the **Backup** button.

2. In the window that will open, select the **Backup** section and click the **Create** button.
3. The Backup Task Creation Wizard will be launched. Let us take a closer look at the wizard's steps:
   a. In the **Content** window, select the objects for which backup copies will be created.
   b. In the **Storage** window, select the storage in which backup copies of files will be created.
   c. In the **Schedule** window, specify the conditions for running the task.
   d. In the **Summary** window, enter the name for the new task and confirm the task creation with the settings you have specified.

RUNNING A BACKUP TASK

Backup tasks may be run automatically (by a schedule) or manually. The actual task run mode is displayed in the list of tasks (see the figure below).

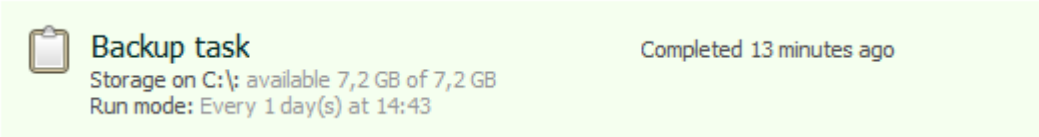


Figure 22. Backup task

Automatic run schedule is configured at the creation of a task; however, it may be subsequently changed.

To run a backup task manually, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Backup** section.
3. From the list in the right part of the window, select the task which should be executed, and click the **Run** link.

   The line of the task you have selected displays the time elapsed since the beginning of the task run. Task run may be paused or cancelled by using respective buttons in the top part of the window.

   Task execution results in creating an archive of current backup copies in the storage.

SEARCHING FOR BACKUP COPIES

To search for backup copies in a storage, you can use the filter and the search field.

Backup copy filter allows displaying only the copies which conform to the search criteria you have specified:

- In the **Archive** dropdown list, select the name of the task which has resulted in creating an archive with the required backup copies, when executed.
- In the **Date** field, specify the date when the archive with the required backup copies has been created.
- From the **Category** dropdown list, select the file types for which backup copies should be found.

You can find a backup copy in the archive, by entering its name in the search field.

To display the backup copies of files which have not been included into the list of files subject to backup at the last execution of the task (e.g., which have been deleted from the computer), check the **Show deleted files** box.

To filter backup copies, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Restore** section.
3. In the left part of the window, select the search criteria from the dropdown lists of the filter. As a result, in the right part of the window, the list will only contain backup copies that meet the specified conditions.

To find a backup copy by its name, please do the following:

1. Open the main application window and click the click the **Backup** button.
2. In the window that will open, select the **Restore** section.
3. In the **Search** field in the left part of the window, enter the full name of a file or a part of it. As a result, in the right part of the window, the list will only contain the backup copies of files whose names start with the characters entered.

VIEWING BACKUP COPY DATA

Before restoring data, you can view the contents of the selected version of backup copy. To do so, you can open the latest version or select a version based on the date specified.

To open the most recent file version, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Restore** section.
3. Select the storage where the required backup copies are located and click the **Restore data** button.
4. In the left part of the **Restore data from storage** window, select an archive.
5. In the right part of the window, select the required file from the list and click the **Open** button.

To open a file version based on the specified date, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Restore** section.
3. Select the storage where the required backup copies are located and click the **Restore data** button.
4. In the left part of the **Restore data from storage** window, select an archive.
5. In the right part of the window, select the required file from the list and click the **Versions** button.
6. In the **File versions** window that will open, select the required date and click the **Open** link.

RESTORING DATA

The data may be restored from the backup copies of files, if necessary. Backup procedure is only available for connected storages. Being restored, data from backup copies are saved into the folder you have selected.

Files may be restored in various ways:

- restore the most recent file version;

- select a version to restore by date.

To restore the most recent file version, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Restore** section.
3. Select the storage where the required backup copies are located and click the **Restore data** button.
4. In the left part of the **Restore data from storage** window, select an archive.
5. In the right part of the window, select the files you need to restore. To do so, check the boxes next to the required files. To select all files, click the **Select all** button in the bottom part of the list. Click the **Restore** button in the top part of the window.
6. In the **Restore** window that will open, select the location to save restored files and the condition of saving if files' names coincide. Click the **Restore** button.

To select the required file version, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, select the **Restore** section.
3. Select the storage where the required backup copies are located and click the **Restore data** button.
4. In the left part of the **Restore data from storage** window, select an archive.
5. In the right part of the window, select the file whose version you want to specify. To do so, check the box next to the file you need. Click the **Versions** button in the top part of the window.
6. In the **File versions** window that will open, select the date of the version you need to restore, and click the **Restore** link.
7. In the **Restore** window that will open, select the location to save restored files and the condition of saving if files' names coincide. Click the **Restore** button.

VIEWING EVENT REPORT

Each event related to data backup and restore is displayed in the report.

To get a backup module report, please do the following:

1. Open the main application window and click the **Backup** button.
2. In the window that will open, click the **Report** button in the top part of the window.
3. In the **Report** window that will open, specify the event display settings.

MY PARENTAL CONTROL

My Parental Control allows to control different users' actions on the local computer and in the network. This module grants an ability to limit the access to resources and applications, as well as view reports on the actions of users.

At the moment more and more children and teenagers have access to computer and Internet resources. This fact raises a problem of security, since working and messaging on the Internet is linked to a number of threats. Among them:

- accessing web sites that can lead to wasting time (chat rooms, games) or money (e-stores, auctions);
- accessing web resources aimed at adult audience (that contain porn, extremist materials involving arms, drugs and violence issues etc.);
- downloading files infected by harmful programs;
- computer and Internet overuse, which can be harmful to health;
- contacting unfamiliar persons who under the semblance of peers can steal user's personal data (real name, address, hours when nobody's at home etc.).

Parental control allows to lower the risks related to computer and Internet usage. To ensure lowering these risks, the module uses the following features:

- restricting computer and Internet access time;
- creating lists of web sites allowed and blocked for access as well as selecting categories of web sites content not recommended for viewing;
- enabling safe search mode;
- limiting downloading files from the Internet;
- creating lists of contacts allowed or blocked for intercourse;
- viewing messaging text;
- forbidding certain personal data transfer;
- searching for key words in messaging texts (the number of key words found is displayed in the **Reports** section);
- creating lists of applications allowed and blocked for launch as well as timely restrictions for allowed applications running.

Every restriction is enabled separately, which allows to adjust Parental Control for different users. For each user account you can view reports that display events in controlled categories for the chosen period.

IN THIS SECTION:

ENABLING AND CONFIGURING PARENTAL CONTROL

You need to perform the authentication procedure to begin managing the component. After you have entered the name and the administrator password, you can enable, pause or disable Parental Control, as well as modify its settings.

When the component is enabled, you can enable and configure various functions of Parental Control for individual accounts. If the component is disabled, no control is being performed.

- *To enable Parental Control, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Users** section. Click the **Enable** link.

- *To pause Parental Control, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Users** section. Click the **Pause** link.
  3. In the **Pause Parental Control** window, select the mode of operation resuming.

  You can also pause or resume Parental Control via Kaspersky PURE main window.

- *To configure Parental Control for an account, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that opens, select the **Users** section, select the account for which Parental Control should be configured, and click the **Configure** button.
  3. In the window that will open, select the component on which you need to impose restrictions, and specify the control settings.

To configure an alias and an image for an account, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that opens, select the **Users** section, select the account for which display settings should be configured, and click the **Configure** button.
3. In the window that will open, in the **Additional** section, select the **Display** component. Enter an alias for the account and select an image to display.

SEE ALSO:

Saving and downloading Parental Control settings 196

LIMITING TIME OF INTERNET ACCESS

You can limit the time which the user spends on the Internet. To do this, you can configure Internet access (certain days of the week and hours when access is allowed or blocked), and also limit the overall time spent on the Internet.

You can view Internet access statistics for each user account on the selected computer as well as a detailed report on the events.

To limit time of Internet access, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
3. In the window that will open, in the **Internet** section select the **Usage** component.
4. In the **Control using the Internet** window that will open, check the **Enable** box and specify time restrictions.

To view brief statistics, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

   The brief statistics for Internet usage for the selected user account is displayed in the **Internet** section.

To obtain a detailed report, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
3. In the window that will open, in the **Internet** section select the **Usage** component.

   In the **Usage** window that will open, a detail report will be displayed.

You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

ACCESS TO WEB SITES

You can set restrictions on certain web resources access depending on their content. To do this, you should create lists of allowed and blocked web pages, as well as choose the categories of web sites, access to which should be blocked.

You can view web sites access statistics for each user account on the selected computer as well as a detailed report on the events.

To restrict the time of web resource access, do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
3. In the window that will open select the **Internet** section and then **Access to web sites** component.
4. In the **Control access to web sites** window that will open, check the **Enable** box and impose the restrictions on access to websites.

   On the **Blocked web addresses** and **Allowed web addresses** tabs, you can enter the addresses of allowed and blocked web sites. On the **Not recommended** tab, you can choose the categories of web sites, access to which should be blocked.
5. In the **Action** dropdown list, select a default action for web sites not included in the list of allowed web sites.

> If you have selected blocking web sites not included in the list of allowed web sites as a default action, add the address of the proxy server to the list of **Allowed web addresses** to connect to the Internet using a proxy.

To view brief statistics, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

   Brief statistics on browsed web sites for the selected account will be displayed in the **Internet** section.

To obtain a detailed report, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
3. In the window that will open select the **Internet** section and then **Access to web sites** component.

   In the **Access to web-sites** window that opens, a detailed report will be displayed.

You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

DOWNLOADING FILES FROM THE INTERNET

You can restrict file types that can be downloaded.

You can view statistics for downloaded and blocked files for each user account on the selected computer as well as a detailed report on the events.

To restrict downloading files from the Internet, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
3. In the window that will open, in the **Internet** section select the **Downloading files** component.
4. In the **Control downloading files from the Internet** window that will open, check the **Enable** box and select the file categories that should be allowed to download.

To view brief statistics, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

   Brief statistics for downloading files from the Internet for the selected account will be displayed in the **Internet** section.

To obtain a detailed report, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
3. In the window that will open, in the **Internet** section select the **Downloading files** component.

   A detailed report will be displayed in the **Downloading files** window that will open.

You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

SAFE SEARCH MODE

Some search engines strive to protect users from inappropriate web sites content. To do this, during web sites indexing they use some key words and phrases, web sites addresses and categories. To enable safe search mode, the following categories of web sites are excluded from the search: porn, drugs, violence and other sites aimed at adult audience.

Parental Control allows to switch on the secure search mode for the following search engines simultaneously:

- Google;
- Bing.com.

To switch on the safe search mode, please do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
3. In the window that will open, in the **Internet** section, select the **Safe search** component.
4. In the **Control search results** window that will open, check the **Enable** box.

INSTANT MESSAGING

Controlling instant messaging means controlling correspondence contents and contacts with which the messaging is allowed. You can create lists of allowed and blocked contacts, specify key words (see section "Key words search" on page. 194) that all incoming messages will be checked for and also enter personal data (see section "Sending personal data" on page 193) prohibited to be sent.

If messaging with a contact is prohibited, then all messages addressed to this contact or received from it will be blocked. Information on blocked messages and key word presence in messages is displayed in the report. In the full report you can see massage history for each contact.

Messaging control has the following restrictions imposed:

- If the IM client was started before Parental Control, messaging control will not be carried out until the IM client is restarted.
- When using HTTP proxies, messaging control will not be carried out.

The current version of Parental Control ensures the control over communication via the following IM clients:

- ICQ;
- QIP
- Windows Live Messenger (MSN);
- Yahoo Messenger;
- GoogleTalk;
- mIRC;
- Mail.Ru Agent;
- Psi;
- Miranda;

Some IM clients use encrypted connection. To control messaging via such programs, you will need to enable the scan of encrypted connections (see page 170).

To restrict instant messaging contacts, do the following:

1. Open the main application window and click the **Parental Control** button.
2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
3. In the window that will open, in the **Messaging** section, select the **IM messaging** component.
4. In the **Control instant messaging** window that will open, check the **Enable** box.
5. On the **Allowed** and **Blocked** tabs, create lists of allowed and blocked contacts.
6. In the **Action** dropdown list, select the default action for contacts not included in your lists.

You can also allow or block communication with the contact you have selected from the detailed report on events for that account.

- *To view brief statistics, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

     In the **Messaging** section, brief instant messaging statistics for the selected user account will be displayed.

- *To obtain a detailed report, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
  3. In the window that will open, in the **Messaging** section, select the **IM messaging** component.

     In the **Instant messaging** window that will open, a detailed report will be displayed.

  You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

SENDING PERSONAL DATA

You can forbid sending data that contain personal information. To do this, create a list of records that contain confidential data (for instance, home address, phone number etc.).

The attempts to send data from the list are blocked and the information on the blocked messages is displayed in the report.

- *To block certain data sending:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
  3. In the window that will open, in the **Messaging** section, select the **Personal data** component.
  4. In the **Control sending personal data** window that will open, check the **Enable** box. Add the record to the list of data forbidden to be sent by clicking the **Add** link.

- *To view brief statistics, please do the following:*

  1. Open themain application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

     Brief statistics for personal data transfer for the selected account will be displayed in the **Messaging** section.

- *To obtain a detailed report, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
  3. In the window that will open, in the **Messaging** section, select the **Personal data** component.

     A detailed report will be displayed in the **Personal data** window that will open.

You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

KEY WORDS SEARCH

You can control key words presence in the instant messaging.

Any key words from the list found in messages are mentioned in the report.

If IM control (see section "Instant messaging" on page 192) is disabled, key words are not searched for, either.

- *To enable key words control in the messaging, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
  3. In the window that will open, in the **Messaging** section, select the **Key words** component.
  4. In the **Control using key words** window that will open, check the **Enable** box. Add the record to the list of key words that are controlled in messaging, by clicking the **Add** link.

- *To view brief statistics, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

     Brief statistics for the key words in messages for the selected user account is displayed in the **Messaging** section.

- *To obtain a detailed report, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
  3. In the window that will open, in the **Messaging** section, select the **Key words** component.

     A detailed report will be displayed in the **Key words** window that will open.

     You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

LIMITING COMPUTER USAGE TIME

You may create a schedule of user access to the computer (weekdays and hours during the day), as well as limit total computer usage time per day.

You can view computer access statistics for each user account on the selected computer as well as a detailed report on the events.

- *To limit daily computer usage:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
  3. In the window that will open, in the **Computer** section, select the **Usage** component.
  4. In the **Control using the computer** window that opens, check the **Enable** box and specify time restrictions.

- *To view brief statistics, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

     Brief statistics on using computer for the selected account will be displayed in the **Computer** section.

- *To obtain a detailed report, please do the following:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.
  3. In the window that will open, in the **Computer** section, select the **Usage** component.

     In the **Usage** window that will open, a detail report will be displayed.

  You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

RUNNING APPLICATIONS AND GAMES

You can allow or block certain applications and games launch, as well as limit allowed applications launch by time.

You can view applications and games launch statistics for each user account on the selected computer as well as a detailed report on the events.

- *To restrict applications and games launch:*

  1. Open the main application window and click the **Parental Control** button.
  2. In the window that will open, select the **Users** section, select a user account, for which a restriction should be created, and click the **Configure** button.
  3. In the window that will open, in the **Computer** section, select the **Running applications** component.
  4. In the **Control running applications** window that will open, check the **Enable** box.
  5. Create lists of applications allowed and blocked for running on the **Allowed** and **Blocked** tabs, and set the run schedule for allowed applications.

- *To view brief statistics, please do the following:*

  1. Open the main application window and click the **Parental Control** button.

2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report.

   Brief statistics on the launch of applications and games for the selected account is displayed in the **Computer** section.

To obtain a detailed report, please do the following:

1. Open the main application window and click the **Parental Control** button.

2. In the window that will open, select the **Reports** section and in the dropdown menu select the user account for which you want to see the report. Click the **Detailed report** link.

3. In the window that will open, in the **Computer** section, select the **Running applications** component.

   A detailed report will be displayed in the **Running applications** window that will open.

> You can also open the detailed report in the **Users** section, by clicking the **Detailed report** button.

SAVING AND DOWNLOADING PARENTAL CONTROL SETTINGS

If you have configured Parental Control for an account, you can save the settings as a file. You can import the settings from this file for quick configuring in the future. Additionally, you can apply control settings of another account or use a configuration template (preconfigured set of rules for various types of users depending on their age, experience, and other parameters).

After the import is completed, you can always modify the settings that you have selected for an individual account.

To save the control settings into a file, please do the following:

1. Open the main application window and click the **Parental Control** button.

2. In the window that opens, select the **Users** section, select the account for which Parental Control settings should be saved, and click the **Configure** button.

3. In the window that will open, click the **Save settings** link in the top part of the window and save the configuration file.

To load the control settings from a file, please do the following:

1. Open the main application window and click the **Parental Control** button.

2. In the window that opens, select the **Users** section, select the account for which Parental Control settings should be downloaded, and click the **Configure** button.

3. In the window that will open, click the **Load settings** link in the top part of the window.

4. In the **Load control settings** window that will open, select the **Configuration file** option and specify the file location.

To apply the settings of a different account, please do the following:

1. Open the main application window and click the **Parental Control** button.

2. In the window that opens, select the **Users** section, select the account for which Parental Control settings should be applied, and click the **Configure** button.

3. In the window that will open, click the **Load settings** link in the top part of the window.

4. In the **Load control settings** window that opens, select the **Another user** option and specify the account whose settings you want to use.

To use a configuration template, please do the following:

1. Open the main application window and click the **Parental Control** button.

2. In the window that opens, select the **Users** section, select the account for which predefined Parental Control settings should be used, and click the **Configure** button.

3. In the window that will open, click the **Load settings** link in the top part of the window.

4. In the **Load control settings** window that opens, select the **Template** option and specify the template whose settings you want to use.

MY SYSTEM TUNE-UP

Ensuring computer's security is a difficult task that requires the expertise in operating system's features and in ways of exploiting its weak points. Additionally, volume and diversity of information about system security makes its analysis and processing difficult.

To facilitate the solving of specific tasks of providing computer security, a set of wizards and tools was included in the Kaspersky PURE package:

- Browser Configuration Wizard (see page 198), performing the analysis of the Microsoft Internet Explorer's settings and evaluating them, primarily, in relation to the security.
- System Restore Wizard (see page 199), eliminating traces of a malware object's presence in the system.
- Rescue Disk Creation Wizard (see page 199), restoring the system's operability after a virus attack, or if the system files of the operating system are corrupted, and it cannot be rebooted as it was.
- Data Deletion Wizard (see page 202), ensuring deletion of confidential data without any opportunity of restoring them in the future.
- Unused Data Clearing Wizard (see page 203), deleting temporary and unused files from your computer and optimizing the system's functioning.
- Privacy Cleaner Wizard (see page 204), searching for and eliminating traces of user's activities in the system.

IN THIS SECTION:

CONFIGURING THE BROWSER

The Browser Configuration Wizard analyzes Microsoft Internet Explorer settings from the perspective of security, since some settings selected by the user or set by default may cause security problems.

The Wizard checks whether the latest software updates for the browser have been installed, and whether its settings contain any potential vulnerabilities which can be used by intruders to inflict damage on your computer. Examples of the analyzed objects:

- **Microsoft Internet Explorer cache**. The cache contains confidential data, from which can be also obtained a history of websites visited by the user. Some malware objects also scan the cache while scanning the disk, and intruders can obtain the user's email addresses. You are advised to clear the cache every time you close your browser.
- **Displaying extensions for files of known formats**. One option for Windows Explorer is to hide file extensions. Many malware objects use double extension, in which case the user can only see a part of the filename without

the real extension. This scheme is often used by intruders. We recommend that you enable displaying extensions for files of known formats.

- **The list of trusted sites**. Malware objects can add links to intruder's websites to this list.

Close all Microsoft Internet Explorer windows before starting the diagnostics.

After the review is complete, the wizard analyzes the information to evaluate whether there exist browser settings posing security problems that require immediate attention. It will then compile a list of actions to be performed in order to eliminate the problems. These actions are grouped by categories based on the severity of the problems detected.

Once the Wizard is complete, a report will be generated which can be sent to Kaspersky Lab for analysis.

Note that some settings may lead to problems with displaying certain sites (for example if they use ActiveX controls). This problem can be solved by adding these sites to the trusted zone.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. In the **Security+** section, click the **My System Tune-Up** button.
3. In the window that will open, click the **Tune Up your Browser Settings** button.

RESTORING AFTER INFECTION

The System Restore Wizard eliminates the traces of actions by malware objects in the system. Kaspersky Lab recommends that you run the wizard after the computer has been disinfected, to make sure that all threats and damage due to the infections have been fixed. You can also use the wizard if you suspect that your computer is infected.

The wizard checks whether there are any changes to the system, such as: access to the network is blocked, known format file extensions are changed, the toolbar is blocked etc. Such damage can be caused by actions of malicious programs, system failures or even incorrect operation of system optimization applications.

After the review is complete, the wizard analyzes the information to evaluate whether there is system damage which requires immediate attention. Based on the review, a list of actions necessary to eliminate the problems is generated. These actions are grouped by categories based on the severity of the problems detected.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. In the **Security+** section, click the **My System Tune-Up** button.
3. In the window that will open, click the **System Restore** button.

RESCUE DISK

Kaspersky PURE includes a service that allows creation of a rescue disk.

Rescue Disk is designed to scan and disinfect infected x86-compatible computers. It should be used when the infection is at such level that it is impossible to disinfect the computer using anti-virus applications or malware removal utilities (such as Kaspersky AVPTool) run under the operating system. In this case, a higher degree of efficiency of the disinfection is achieved since malware programs do not gain control when the operating system is being loaded.

Rescue disk is an .iso file based on the Linux core that comprises the following:

- system and configuration Linux files;
- a set of operating system diagnostic utilities;
- a set of additional tools (file manager, etc.);
- Kaspersky Rescue Disk files;
- files containing anti-virus databases.

A computer with corrupted operating system is booted from a CD / DVD-ROM device. To do so, the computer should be equipped with suitable device.

To create a rescue disk, please do the following:

1. Open the main application window.
2. In the **Security+** section, click the **My System Tune-Up** button.
3. In the window that will open, click the **Create Rescue Disk** button to run the disk creation wizard.
4. Follow the wizard instructions.
5. Using the file provided by the wizard, create a boot CD/DVD. To do so, you can use any CD / DVD burning application, such as Nero.

SEE ALSO:

CREATING THE RESCUE DISK

Rescue disk creation means the creation of a disk image (ISO file) with up-to-date anti-virus databases and configuration files.

The source disk image serving as base for new file creation can be downloaded from Kaspersky Lab server or copied from a local source.

The image file created by the wizard will be saved in the "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk*" folder (or "*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*" – for Microsoft Vista) named as *rescuecd.iso*. If the wizard has detected an ISO file created earlier in the specified folder, you can use it as original disk image by checking the **Use existing ISO file** box, and jump to Step 3 – image update. If the wizard has not detected any image file, this box is not available.

Rescue disk is created by a wizard that consists of the series of boxes (steps) browsed with the **Back** and **Next** buttons; the wizard finishes its activity by clicking the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

SEE ALSO:

BOOTING THE COMPUTER USING THE RESCUE DISK

If the operating system cannot be booted as a result of a virus attack, use the rescue disk.

You will need the boot disc image file (.iso) to load the operating system. You can download an ISO file from Kaspersky Lab server, or update the existing one.

Let us take a closer look at the rescue disk functioning. When loading the disk, the following operations are under way:

1. Automatic detection of the computer's hardware.
2. Searching file systems on hard drives. File systems detected will be assigned names starting with *C*.

   Names assigned to hard drives and removable devices may not match names assigned to them by the operating system.

   If the operating system of the computer being loaded is in sleeping mode, or its file system has the *unclean* status due to an incorrect shutdown, you will be offered to choose whether you wish to mount the file system or restart the computer.

   File system mounting may result in its corruption.
3. Searching the Microsoft Windows swap file *pagefile.sys*. If it is missing, the volume of the virtual memory is limited by the size of the RAM.
4. Selecting the localization language. If the selection has not been done after a lapse of time, then the English language will be set by default.
5. Searching (creating) the folders for anti-virus databases, reports, quarantine storage, and additional files. By default, the folders of Kaspersky Lab's applications, installed on the infected computer (*ProgramData/Kaspersky Lab/AVP8* – for Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* - for earlier versions of Microsoft Windows) will be used. If such application folders cannot be found, an attempt to create them will be made. If those folders have not been found, and they cannot be created, the *kl.files* folder will be created on a system disk.
6. Trying to configure network connections based on data found in system files of the computer being loaded.
7. Loading graphical subsystem and starting Kaspersky Rescue Disk.

In system rescue mode only virus scan tasks and database updates from a local source are available, as well as update rollback and viewing of statistics.

To load the operating system of an infected computer, please do the following:

1. In the BIOS settings, enable bootingfrom CD/DVD-ROM (for detailed information please refer to the documentation for the motherboard installed on your computer).
2. Insert the CD/DVD with rescue disk image into the CD/DVD drive of an infected computer.
3. Restart your computer.

Further the boot continues according with the algorithm described above. For more details on the features of rescue disk please refer to Kaspersky Rescue Disk Help.

SEE ALSO:

Creating the rescue disk.....200

PERMANENTLY DELETE DATA

Data security is ensured not only by the protection against viruses, Trojans and other types of malware, but also by the protection against unauthorized restoration of deleted information.

Deleting data with the standard Microsoft Windows tools cannot ensure safety and prevent possible restoration. The data do not disappear from the hard drive when deleted. They are stored in the disk sectors and marked as free. The file record in the file table is the only thing which is deleted. Formatting data storage media (such as hard disk drives, flash cards, or USB cards) cannot guarantee total data deletion either. It is considered that data can only be deleted after multiple re-recording. However, even in this case, information may be restored using high-performance software tools.

Kaspersky PURE includes the Permanent Data Deletion Wizard. This wizard allows deleting confidential data without any opportunity of restoring and using them by hackers. Permanent data deletion precludes from restoring information using common software tools. The wizard is applicable both to small-sized objects and to large-sized ones (up to several gigabytes).

Depending on the current conditions, the wizard supports deletion of data from the following data storage media:

- local disk drives – deletion is possible if the user has the rights required for recording and deleting information;
- any removable drives or other devices that can be detected as removable drives (such as floppy disks, flash cards, USB cards, or cell phones). Data can be deleted from a flash card if the mechanic protection from rewriting (Lock mode) is disabled.

Before starting the permanent deletion, the application finds out if data can be deleted from the selected data storage medium. The deletion procedure can only be carried out if the selected data storage medium supports data deletion. Otherwise, the data cannot be deleted permanently.

Such objects as a file or a folder can be deleted. To avoid unintentional deletion of useful data, you can select only one object for deletion, although the folder you have selected for deletion may contain several files or nested folders.

The folder you have selected for deletion may contain system files that cannot be deleted on penalty of operating system failures. When system files and folders are found among the chosen data, the wizard requests additional confirmation for their deletion.

Methods for permanent deletion of personal data are standardized. They are based on multiple rewriting deleted information with ones, zeroes, or random symbols. Deletion speed and quality may vary depending on the number of cycles.

You are offered to select one of the following data deletion standards:

- **Quick delete**. Deletion process consists of two cycles of data rewriting: writing zeroes and pseudorandom numbers. The main advantage of this algorithm is performance speed. Two cycles are enough to complicate the operations of data restoration tools. Even if the file itself will be restored, the data will turn out to be annihilated.
- **GOST state standard P 50739-95, Russian Federation**. The algorithm carries out one rewriting cycle using pseudorandom numbers and protects the data from restoration with common tools. This algorithm corresponds to protection class 2 out of 6 total, according to the State Technical Commission classification.
- **VSITR standard, Germany**. The algorithm carries out seven rewriting cycles. The algorithm is considered reliable but it requires more time for execution.
- **Bruce Schneier algorithm**. The process consists of seven rewriting cycles. The method differs from VSITR by its rewriting sequence. This enhanced method of data deletion is considered the most reliable.

- **NAVSO P-5239-26 (MFM) standard, USA** and **NAVSO P-5239-26 (RLL) standard, USA**. The algorithm carries out three rewriting cycles. The standards differ from one another by their sequences of data deletion.

- **DoD 5250.22-M standard, USA**. The algorithm carries out three rewriting cycles. It is considered a reliable method of protection against people who do not have special tools but, however, data are successfully restored in many cases.

You can only delete the data that you can access under your personal account. Before deleting the data, make sure that the file or the folder is not opened, or it is not in use by other applications.

To start the wizard:

1. Open the main application window.
2. In the **Security+** section, click the **My System Tune-Up** button.
3. In the window that will open, click the **Permanently delete data** button.
4. In the **Permanently delete data** window that will open, select an object using the **Browse** button, then select an object to delete in the **Select folder** window that will open.

   From the **Data deletion method** dropdown list, select the required data deletion algorithm.
5. In the window that will open, confirm the data restoration by clicking the **OK** button. If some files are not deleted, try to delete them again by clicking the **Retry** button in the window that will open. To select another object to delete, click the **Finish** button.

DELETE UNUSED DATA

The system may often accumulate too many temporary or unused files which reduces its performance.

All applications or operating systems create temporary files when started. But some of them remain undeleted when closing the application or operating system. Temporary and unused files often require too large amounts of memory. Additionally, they may be exploited by malicious programs. Unused information includes the following files:

- system event logs, where the names of all active applications are recorded;
- event logs of various applications (such as Microsoft Office, Microsoft Visio, Macromedia Flash Player) or update utilities (such as Windows Updater, Adobe Updater);
- system connection logs;
- temporary files of Internet browsers (cookies);
- temporary files remaining after installation / removal of applications;
- Recycle Bin contents;
- files in the TEMP folder whose volume may grow up to several gigabytes.

Kaspersky PURE includes the Unused Data Clearing Wizard. The wizard's purpose is helping you optimize the system's functioning. Besides the deletion of unused files from the system, the wizard deletes the files which may contain confidential data (passwords, usernames, data from registration forms). However, for complete deletion of such data, we recommend that you use the Privacy Cleaner Wizard (see page 204).

When cleaning the system, some files (such as Microsoft Windows log file, Microsoft Office event log) may be in use by the system. In order to delete these files the wizard will suggest that you restart the system.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. In the **Security+** section, click the **My System Tune-Up** button.
3. In the window that will open, click the **Delete unused data** button.

PRIVACY CLEANER WIZARD

Many of a computer user's actions are registered in the system. The following data is saved in this case:

- Histories containing information:
  - about visited websites;
  - about applications launch;
  - about search requests;
  - about opening / saving files by different applications.
- Microsoft Windows system log records.
- Temporary files etc.

All these sources of information about the user's activity may contain confidential data (including passwords) and may become available to intruders for analysis. Frequently, the user has insufficient knowledge to prevent information being stolen in this way.

Kaspersky PURE includes the **Privacy Cleaner Wizard**. This wizard searches for traces of user's activities in the system as well as for operation system settings, which contribute to storing of information about user's activity.

Information about a user's activity in the system is constantly accumulated. The launch of any file, or the opening of any document will be logged. The Microsoft Windows system log registers many events occurring in the system. For this reason, repeated running of the **Privacy Cleaner Wizard** may detect activity traces which were not cleaned up by the previous run of the wizard. Some files, for example the Microsoft Windows log file, may be in use by the system while the wizard is attempting to delete them. In order to delete these files the wizard will suggest that you restart the system. However, during the restart these files may be re-created and detected again as activity traces.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

To start the wizard:

1. Open the main application window.
2. In the **Security+** section, click the **My System Tune-Up** button.
3. In the window that will open, click the **Erase Your Activities History** button.

MY VIRTUAL KEYBOARD

When working on your computer, the cases frequently occur when it is required to enter your personal data, or username and password. For instance, when registering on Internet sites, using online stores etc.

There is a danger that this personal information will be intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

My Virtual Keyboard prevents the interception of data entered at the keyboard.

My Virtual Keyboard cannot protect your personal data if the website, that required entering such data, has been hacked, since in this case the information will be obtained directly by the intruders.

Many of the applications classified as spyware have the functions of making screenshots which then are transferred to an intruder for further analysis and for stealing the user's personal data. My Virtual Keyboard prevents the personal data being entered, from being intercepted with the use of screenshots.

My Virtual Keyboard only prevents the interception of privacy data when working with Microsoft Internet Explorer and Mozilla Firefox browsers.

To start using My Virtual Keyboard:

1. Open themain application window and click the **My Virtual Keyboard** button.

2. Enter the required data by pressing the buttons on the virtual keyboard. Make sure that data is entered in the correct field. When you press function keys (**Shift**, **Alt**, **Ctrl**) on the virtual keyboard, that particular mode will be fixed: for example, when you press **Shift** all symbols will be entered in the upper case. To exit the special mode, press the same functional key again.

You can switch the language for the virtual keyboard using the key combination **Ctrl** + right-clicking **Shift**, or **Ctrl** +right-clicking **Left Alt**, depending on the settings selected.

MY ENCRYPTION

Data encryption is designed for protecting confidential information against unauthorized access. At that, encrypted information is stored in a special container.

Container is an encrypted object created by the user with the Data encryption function. Files and folders are moved into the container. To access the data stored in the container, you should enter a password. Additionally, Kaspersky PURE must be installed on the computer.

The container should be connected in order to work with the data. At that, the system requests a password for access. When connected, the container is displayed in the system as a virtual removable drive onto which you can copy or move files and folders with data.

IN THIS SECTION:

CREATING A CONTAINER

To store encrypted data, you need to create a container. You can create a container on a local or removable drive.

A container can be created using the wizard. When creating a container, you need to specify its name, size, access password, and container file location.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

You can also specify an existing container if it is unavailable on the computer you are currently using (for example, after the operating system is reinstalled, or if the container is copied from another computer). In this case, the container appears in the list but it remains disabled. The container should be connected in order to work with data (see section "Connecting and disconnecting container" on page 207).

To create a container, please do the following:

1. Open the main application window and click the **My Encryption** button.
2. In the window that will open, click the **Create container** button.
3. The Encrypted Container Creation Wizard will be started. Let us take a closer look at the wizard's steps:
    a. Enter the name of the container, as well as its size and access password in the **Main settings** window.
    b. Specify the location of the container file in the **Location** window.

c. Select a letter of virtual drive to connect this container, specify the advanced settings, if necessary, and confirm creation of the container with the specified settings in the **Summary** window.

To specify an existing container, please do the following:

1. Open the main application window and click the **Data encryption** button.
2. In the window that will open, click the **Select container** button.
3. In the window that will open, specify the location of the container file.

CONNECTING AND DISCONNECTING CONTAINER

When created, a container is connected automatically. If an existing container is specified, it is disconnected by default. You should connect the container to store data. You can do that via Kaspersky PURE interface or the Microsoft Windows context menu.

If the container is stored on a removable medium, you can configure the automatic connection of the medium when being connected.

A connected container is available to all computer accounts as a removable drive in the list of devices, so we recommend that you disconnect the container when taking no actions on the data. You can do that via Kaspersky PURE interface or the Microsoft Windows context menu.

To connect a container via the application interface, please do the following:

1. Open the main application window and click the **Data encryption** button.
2. In the window that will open, click the **Connect** button.
3. In the window that will open, enter the container connection settings and confirm the connection.

To connect a container via the context menu, please do the following:

1. Right-click the container file icon or the desktop shortcut to open the context menu (see section "Creating shortcut to access the container" on page 209).
2. Select the **Connect container** item from the menu that will open.

To connect the container automatically at the connection of a medium, please do the following:

1. Open the main application window and click the **Encryption** button.
2. In the window that will open, select a connected container and click the **Configure** button.
3. In the window that will open, check the **Connect container automatically** box.

To disconnect a container via the application interface, please do the following:

1. Open the main application window and click the **Data encryption** button.
2. In the window that will open, click the **Disconnect** button.

To disconnect a container via the context menu, please do the following:

1. Right-click to open the context menu of a file, or that of a desktop shortcut of access to container (see section "Creating shortcut to access the container209" on page), or that of a removable drive.
2. Select the **Disconnect container** item from the menu that will open.

ADDING FILES INTO CONTAINER

When connected (see section "Connecting and disconnecting container" on page 207), the container is displayed as a virtual removable drive within the system, being available to all the users of the operating system. You can open the container and place files and folders in it if you need to store them in encrypted form.

To ensure data security, we recommend that you disable the container after finishing the operations. When the container is disconnected, you need to enter a password to obtain access to the encrypted data.

- *To open a container via the application interface:*

  1. Open the main application window and click the **Encryption** button.
  2. In the window that will open, select a connected container and open it with a double-click.
  3. Place in it the data you want to encrypt.

- *To open a container via the context menu, please do the following:*

  1. Right-click to open the context menu of a connected container file or shortcut to access the container (see section "Creating shortcut to access the container" on page 209) on the desktop.
  2. Select the **Open container** item from the menu that will open.

CONFIGURING CONTAINER

You can change the container's name and the access password.

You can modify the settings for a disconnected container only.

- *To rename a container, please do the following:*

  1. Open the main application window and click the **Data encryption** button.
  2. In the window that will open, select a container and click the **Configure** button.
  3. In the window that will open, enter the password to obtain access to the container.
  4. In the **Container settings** window that will open, specify the new name of the container.

- *To change the password for the container, please do the following:*

  1. Open the main application window and click the **Encryption** button.
  2. In the window that will open, select a container and click the **Configure** button.
  3. In the window that will open, enter the password to obtain access to the container.
  4. In the **Container settings** window that will open, click the **Change password** link.
  5. In the **Change password** window that will open, fill in all fields.

CREATING SHORTCUT TO ACCESS THE CONTAINER

To ease the management of data, you can create a desktop shortcut to access the container. You can use the shortcut to quickly open, connect and disconnect the container irrespective of the actual location of the container file (if you have access to this file from your computer).

You can create a shortcut during container creation or at any time after the creation of the container.

To create a shortcut to access the container, please do the following:

1. Open the main application window and click the **Data encryption** button.
2. In the window that will open, select a disconnected container and click the **Configure** button.
3. In the window that will open, click the **Create desktop shortcut** link.

MY PASSWORD MANAGER

Password Manager stores and protects all your personal data (e.g. passwords, user names, Internet pager accounts, contacts, phone numbers, etc.). Password Manager sticks passwords and accounts to Microsoft Windows applications and web pages for which they are used. All information is stored in encrypted form in the Password Database, access to which is protected by a Master Password. Personal data is easily accessible if the Password Database is unlocked. After launching a web page or application, Password Manager automatically enters the password, user name and other personal data. Thus, you need not remember all the passwords, you only need to remember one password.

Password Manager loads by default at system startup. This component is built in into the application which allows personal data to be managed directly from the application window.

Password Manager monitors the actions of applications with passwords and prevents the interception and theft of personal data. This component checks applications that use passwords or request them from other applications, before asking you to allow or forbid a suspicious action.

Additionally, Password Manager can:

- save and use your passwords (see page 221);
- find accounts, passwords, user names and other personal information in the Password Database (see page 222);
- generate secure passwords (see page 239) when registering new accounts;
- save all passwords on removable device;
- restore Password Database from backup copy (see page 224);
- protect passwords from unauthorized access (see page 214).

To launch Password Manager, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.

IN THIS SECTION:

MY PASSWORD MANAGER INTERFACE

The Password Manager interface is simple and convenient. In this chapter, we shall take a closer look at the main principles of working with the application.

Password Manager has plug-ins embedded in applications that require authorization. You can install plug-ins on your own for the browsers you need. Installed plug-ins provide access to Password Manager functions from the application / browser interface.

Password Manager allows using the Password Manager pointer to quickly select an application / web page for automatic input of personal data.

IN THIS SECTION:

NOTIFICATION AREA ICON

Immediately after installing Password Manager, the application icon will appear in the Microsoft Windows taskbar notification area.

Depending on the situation, the Password Manager icon will take the following form:

-  active (green) – Password Manager unlocked, access to personal data granted;
-  inactive (red) – Password Manager locked, personal data inaccessible.

Additionally, the following interface items are accessible by clicking the icon:

- context menu (see page 211);
- main application window (see page 212);
- Password Manager pointer (see page 240).

The context menu is opened by right-clicking the Password Manager icon.

By double-clicking the Password Manager icon, you can lock / unlock the application.

To use the Password Manager pointer, point the mouse cursor on the application icon and wait a few seconds. The Password Manager pointer will be located above the application icon.

CONTEXT MENU OF MY PASSWORD MANAGER

The main application tasks are accessible from the context menu of Password Manager. The Password Manager menu contains the following items:

- **Lock / Unlock** – allowing or forbidding of access to your personal data.
- List of frequently used accounts – quick launch of one of the frequently used accounts. The list is generated automatically based on how frequently the accounts are used. The list is available if it is configured to be displayed in the context menu (see page 227). When the application is first launched, the list will not be available since no record will have been used.
- **Accounts** – view list of all accounts and quickly launch one of them. The number of accounts in the Password Database is specified in brackets.
- **Add an account** – adding a new account to Password Manager.
- **Password Manager** – switching to the main application window (see page 212).
- **Settings** – configure application settings.
- **Password generator** – create passwords.
- **Help** – opening the application's help section.
- **Exit** – close the application. When this option is selected, the application will be unloaded from the computer's RAM.

If the application is not unlocked, access to your personal data will be blocked. In this case, the context menu will only contain the following items: **Unlock**, **Password generator**, **Help**, and **Exit**.

MY PASSWORD MANAGER WINDOW

The main application window can be opened from the Password Manager context menu (see page 211). To do so, select the **Password Manager** item from the application context menu.

You can also set up the launch of the Password Manager main window by double-clicking on the Password Manager icon in the taskbar notification area.

The **Password Manager** window can be divided into two parts:

- in the upper part of the window, you can select Password Manager functions and perform the main tasks;
- the lower part of the window contains a list of all accounts and other personal data, and enables you to manage your personal information.

You can use the search field to find personal data in the Password Database. The search field is located in the bottom part of the main application window.

APPLICATION SETTINGS WINDOW

The settings window in Password Manager can be opened in one of the following ways:

- from the Password Manager context menu (see page 211) – to do so, select the **Settings** item from the Password Manager context menu;
- from the Kaspersky PURE window **–** to do so, in the **Security+** section, click **Password Manager**.

The application settings window consists of two parts:

- the left part of the window contains the list of application functions;
- the right part of the window contains the list of settings for the chosen function, task, etc.

CAPTION BUTTON

The Caption Button enables you to work with personal data from the application / browser window. This button is located in the upper-right corner of the application.

The Caption Button is active  if Password Manager is not locked. Click it to do the following:

- **Add Account** – add a new account.
- **Manage Account** – add a user name / edit the activated account. The menu item is available if the account is activated.
- **Web Accounts** – view the list of all Web accounts and open one of them. The number of accounts in the Password Database is specified in brackets.
- List of frequently used accounts – launch an account from the list. The list is generated automatically based on how frequently the accounts are used. The list is available in the menu if it is additionally configured to be displayed (see page 227).
- **Identities** – view the list of created Identities and select an Identity for the registration form.
- **Help** – switch to the application's help section.

The Caption Button is not active  if Password Manager is locked. In such case, clicking the button will not enable any actions. The inactive button is displayed in the application window if the Caption Button is additionally configured (see page 237).

CONFIGURATION WIZARD

The configuration wizard for the application is launched when Password Manager is started for the first time. Its purpose is to help you perform the initial configuration of Password Manager in accordance with your personal preferences and tasks.

The wizard is presented as a sequence of windows (steps). You can move through the steps by clicking **Next** and **Back** as required. To exit the wizard at any stage, click **Exit**. To complete the wizard, click **Finish**. Now we shall discuss each of the wizard's steps in more detail.

PASSWORD DATABASE MANAGEMENT

The Password Database stores all accounts for applications and web pages with one or several user names, as well as Identities (cards containing, for example, contact details, phone numbers, Internet pager numbers, etc.).

You can use the Password Database if it is unlocked (see page 214). Before entering any changes in the Password Database, it is recommended that you configure Password Database backup (see page 231). If this data is accidentally changed or deleted, use Restore Password Database (see page 224).

You can do the following:

- add (see page 215), change (see page 221), delete (see page 223) personal data;
- import / export (see page 223), restore (see page 224) Password Database.

IN THIS SECTION:

ACCESSING PASSWORD DATABASE

All your personal data is stored in encrypted form in the Password Database. Password Database must be unlocked to use this data. To access the Password Database, select one of the following authorization methods:

- **Master Password protection**. Master Password is used to access the Password Database.
- **USB device**. To access the Password Database, connect any USB device to your computer. When the USB device is disabled, the Password Database is automatically locked.
- **Bluetooth device**. To access the Password Database, connect a Bluetooth device to your computer. When the Bluetooth device is disabled, the Password Database is automatically locked.
- **No authorization**. Access to the Password Database is unprotected.

By default, protection is set by the Master Password, which means that you only need to remember one password.

Master Password is the basic tool that protects your personal data. If you have selected the method of authorization with a device, and the latter has turned out to be unavailable (or lost), you can use the Master Password for accessing your personal data.

By default, Password Manager locks the Password Database when the application is launched and after a specified time (see page 233) during which the computer is not used. The application can only be used if the Password Database is unlocked.

You can also unlock / lock the Password Database in one of the following ways:

- using a USB or Bluetooth device - only for authorization with a USB or Bluetooth device;
- by double-clicking the application icon (see page 236) - the Double-click action in this case should be configured additionally;
- from the context menu of My Password Manager;
- by using the key combination CTRL+ALT+L (see page 229).

To enter the Master Password, use a virtual keyboard that allows passwords to be entered without pressing keys on the keyboard.

To lock an application from the context menu of the application, please do the following:

1. Right-click the Password Manager icon in the taskbar notification area.
2. In the menu that will open, select the **Lock** item.

To unlock the Password Database from the context menu, please do the following:

1. Right-click the Password Manager icon in the taskbar notification area.
2. In the displayed menu, select **Unlock**.
3. Enter the Master Password in the displayed window.

ADDING PERSONAL DATA

Personal data can be added if Password Database is not locked (see page 214). When launching an application / web page, a new account is recognized automatically if it was not found in the Password Database. Following authorization in the application / on the web page, Password Manager can then add personal data to the Password Database.

You can add the following personal data to the Password Database:

- **Account** (see page 215).
- **User name** (see page 219). By default, Password Manager provides the option to create an account with one user name. An additional user name is used when applications or web pages allow multiple user names to be created for accessing their resources.
- **Identities** (see page 220). Used to store data such as sex, date of birth, contact information, phone number, place of work, Internet pager number, homepage address, etc. To separate personal and business information, you can create several identity cards.
- **Group of accounts** (see page 220). Used to organize accounts in the Password Database.

ACCOUNT

Password Manager automatically recognizes a new account if it is not found in the Password Database. After authorization in the application / on the web page, Password Manager offers to save data in the Password Database. You can also add a new account to the Password Database manually.

Account contains the following data:

- user name / several user names;
- password;
- application path / Internet address of web page;
- settings defining relations between the account and the object;
- settings defining how the account is activated;
- comments;
- settings for completing additional fields on the web page.

Password Manager allows using one or several account(s) for the application / website. Based on the path to the application / Internet address of web page, Password Manager allows specifying a scope for each account.

You can add an account in several ways:

- by clicking the Caption Button – to do this, you need to select **Add Account** in the Caption Button menu;
- from the context menu of My Password Manager – to do this, you need to select **Add Account** in the context menu of My Password Manager;
- from the main Password Manager window.

To add a new account:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add account**.
3. In the window that will open, in the **Name** field, enter the name of the new account (e.g. the name of the application / web page).
4. Under the tab **Login information**, enter the user name and password.

   The user name can consist of one or several words. To specify key words (see page 216) for the user name, click  .

   To copy a user name / password to clipboard, click  .

   To create a password automatically, click on the 239**Generate password** link.
5. Under the **Links** tab, specify the path to the program / web page, and specify the account's settings.
6. On the **Manual form edit** tab, modify the settings for populating other fields of the web page, if necessary.
7. If necessary, under the **Comments** tab, enter some explanatory text for the account. To display comments in a notification after activating the account, check the box  **Show comments in the notification**.

KEYWORD SEARCH

To quickly search for personal data in the Password Database, you can use keywords. They are generated for each user name. It is recommended to assign keywords when adding an account (see page 215) / user name (see page 219).

To specify keywords for the user name, please do the following:

1. In the context menu of the application, select **Password Manager**.

2. In the **Password Manager** window under the **Edit** tab, select the user name from the **My Passwords** list and open it for editing by clicking **Edit**.

3. In the displayed window, click  next to the **Login** field and fill in the **Description** field.

   If an account was chosen with one user name, in the **Account with a single Login** window under the **Login information** tab, click  .

ADDING PATH TO PROGRAM / WEB PAGE

Personal data from the account will be automatically entered into the authorization fields of the web page / program. A link is used to define a web page / application. For a web page, it is the address, and for a program, it is the path to the executable file of the application on the computer. Without this data the account will not be sticked to any application / web page.

It is possible to stick the account to a program / web page in the following ways:

- by following the link  in the list of your browser's chosen websites or the list of applications on your computer;
- by manually specifying the path to the application / web page;
- by using the Password Manager pointer.

To check the entered path, launch the application / web page by clicking  .

To select a link for the account, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add account**.
3. In the displayed window, under the **Links** tab, in the field **Link**, click  .
4. In the displayed window, in the field **Link,** enter the path for the application / web page.

   To specify a web page from the list of saved web pages (Favorites), in the **Tabs** list, select a web page and click the **Copy link from Favorites** link. To copy the path to the web page from the browser window, click the **Use path to the linked application** link.

   To select a link for the application, in the field **Link**, specify the path on your computer by clicking  .

To specify the path to the program / web page manually, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add account**.
3. In the displayed window, under the **Links** tab in the field **Link,** enter the path to the program / address of the web page. The address of the web page must begin with http://www.

To enter the path to the program / web page using the Password Manager pointer, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, click **Add account**.
3. In the displayed window, under the **Links** tab, in the field **Link**, enter the path to the program / web page by moving the Password Manager pointer to the program / browser window.

SELECTING A METHOD TO STICK THE ACCOUNT

To determine which account data should be entered automatically at each startup of the application / web page, Password Manager uses the path to the application / Internet address of web page.

Because Password Manager allows using several accounts for a single application / website, you should specify a scope for each account.

Based on the path to the application / Internet address of web page, Password Manager allows creating a scope for any account. Scope may be configured at the account creation (see page 215). You can alter the settings in the future.

Depending on the object (application or website), the way accounts are used varies.

The following options are available for the application:

- Use the account for the application. The account will be used for all application's dialogs which have fields for entering personal data.
- Recognize by window heading. The account will only be used for the given application window.

  For example, one application can use multiple accounts. For different accounts, only the window headings will differ within one application. Password Manager will automatically enter data for the account based on the application window's heading.

The following options for using an account are available for web pages:

- Only for the given web page. Password Manager automatically adds the user name and password to the identification fields on the given web page only.

  For example, if the account is related to a web page with the address http://www.web-site.com/login.html, it will not be valid for other websites, e.g. http://www.web-site.com/pointer.php.
- For websites from a directory. Password Manager automatically adds the user name and password to identification fields for all web pages in the most recent folder.

  For example, if the website address http://www.web-site.com/cgi-bin/login.html was entered, the account will be used for web pages in the *cgi-bin* folder.
- For the website: <third-level domain name and lower>. This account is used for any web page in the domain (third-level domain and lower).

  For example, Password Manager automatically adds identity data for websites: http://www.domain1.domain2.web-site.com/login.html or http://www.domain1.domain2.web-site.com/pointer.php. However, the account will not be used for web pages with addresses that have different fourth-level domains: http://www.domain3.domain2.web-site.com/pointer.php or http://www.domain4.domain2.web-site.com/pointer.php.
- For the website: <name of website>. The account will be used for all web pages with fields for entering user names and passwords.

  For example, Password Manager automatically adds identity cards for web pages: http://www.domain1.domain2.web-site.com/login.html, http://www.domain2.domain2.web-site.com/pointer.php, http://www.domain3.domain2.web-site.com/pointer.php or http://www.domain4.domain2.web-site.com/pointer.php.

To set parameters for using an account, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window, under the **Edit** tab, select the account from the **My Passwords** list, and then open it by clicking **Edit**.
3. In the displayed window, under the **Links** tab, select one of the options for using the account.

AUTOMATIC ACTIVATION OF THE ACCOUNT

By default, automatic activation of the account is enabled. Password Manager only enters the user name and password in the identity fields. You can modify the advanced settings for the account activation (see page 215).

A range of web addresses, for which automatic activation is used, is additionally specified for the web page.

The following options are available for activating the account:

- For the chosen web page. The account is activated only for the given web page.
- For the website. The account is activated on all web pages on the website.

To set automatic activation of the account, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window, under the **Edit** tab, select the account from the **My Passwords** list, and then open it by clicking **Edit**.
3. In the displayed window, under the **Links** tab, select the **Autoactivate account after loading** checkbox.

   Additionally, specify one of the methods to activate the account for the web page.

FILLING IN ADDITIONAL FIELDS

During authorization on a website, other data is often requested in addition to password and user name. Password Manager can automatically fill in additional fields. You can set options for automatic fill-in of additional fields for the account.

It is possible to set options for additional fields if the application path / website address is specified.

To set options for fields, Password Manager temporarily loads the website, and analyzes all the fields and buttons. Fields and buttons are merged into groups for each web page.

Password Manager temporarily saves files and pictures on your computer from the loaded web page.

To set options for additional fields, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window under the **Edit** tab, select the account from the **My Passwords** list and open it for editing by clicking **Edit**.
3. In the window that will open, on the **Manual form edit** tab, click on the **Edit form fields** link.
4. In the **Manual form edit** window that will open, check the box next to the required field / button.
5. Activate the **Value** field for the chosen field / button by double-clicking the mouse and then setting the field values.

   To return to the list of all fields / buttons, click **Edit field**. To delete a value, click **Delete**. To change a value of the field / button once more, click **Edit**.

USER NAME

Multiple user names are often used for certain applications / websites. Password Manager allows multiple user names to be saved for one account. Password Manager automatically recognizes a user name when it is first used and provides the option to add it to an account for an application / website. You can add a new user name manually for an account and then change it (see page 221).

You can add a new user name for an account in the following ways:

- By clicking the Caption Button. To do so, in the Caption Button menu, select the **Manage Account** → **Add login** item.
- From the main application window.

To add a user name for an account, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager**, under the tab **Edit**, select the account from the **My Passwords** list, and then click **Add login**.
3. In the window that will open, enter the user name and the password. The user name can consist of one or several words. To specify keys words for a user name, click  and then fill in the **Description** field.

   To copy a user name / password to clipboard, click  . To create a password automatically, click on the **Generate password** link (see page 239).

IDENTITY

In addition to user name and password, other personal data is often used for registration on the website, e.g. full name, year of birth, sex, email address, phone number, country of residence, etc. Password Manager can store all this data in an encrypted Password Database in the form of Identities. During registration on a new website, Password Manager automatically fills in the registration form using data from a chosen Identity. To save private and business information separately, you can use several identity cards. You can change the identity parameters later (see page 221).

To create an identity card, please do the following:

1. In the context menuof the application, select **Password Manager**.
2. In the **Password Manager** window, under the tab **Edit**, click **Add Identity**.
3. In the window that will open, in the **Name** field, enter the name of the identity.
4. Enter values for the required fields and activate them by double-clicking the mouse.

GROUP OF ACCOUNTS

Using groups of accounts can help organize information in the Password Database. A group consists of a folder with accounts added to it.

Newly created groups are displayed in the Password Manager context menu: the **Accounts** → **<Group name>** item.

To create a group of accounts, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window under the tab **Edit**, click **Add group**.
3. Enter the name of the created folder.
4. Add accounts from the **My passwords** list by dragging them into the created folder.

EDITING PERSONAL DATA

In Password Database, you can change any personal data: account, user name, identity card, or group of accounts. When editing the settings of each element, you can do the following:

- For the account:
  - change the name of the account, the value of the user name, and password – if the account has one user name;
  - change the path to the application / web page which use the account;
  - select the rules for using the account;
  - set automatic activation;
  - edit additional fields in the account;
  - change comments for the account.
- For the user name – change the value of the user name, and password.
- For the Identity – change the name of the Identity, and value of the required fields.
- For the group of accounts – change the name, and icon of the group.

Since Password Manager is embedded in the windows of the applications and web pages for which it is used, you can edit the settings of accounts or user name directly from the application / browser window.

You can change the settings of the account or user name in the following ways:

- From the context menu. To do so, open the application context menu and select the **Accounts** → **<Name of group of accounts>** → **<Account name>** → **Edit Account** item.
- From the main application window.
- By clicking the Caption Button. To do so, open the Caption Button menu and select the **Manage Account** → **Edit Account** item.

To change the field values and parameters of an element from the main window, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window, under the **Edit** tab, select the element from the **My Passwords** list.
3. In the displayed window, modify the settings for the element.

USING PERSONAL DATA

Password Manager sticks accounts to applications / web pages for which they are used. Password Database automatically searches for sticky accounts when applications / web pages are launched. If an account is found, personal data is entered automatically. If there is no sticky account in the Password Database, Password Manager automatically offers you to add one to the Password Database (see page 215).

Some applications / websites can use multiple user names. Password Manager allows several user names to be saved for one account. If a new user name was used during authorization, Password Manager suggests adding it to the account (see page 219) for the application or web page that was launched. When the application / web page is next launched, a window with a list of user's names for this account will appear next to the personal data input fields.

In addition to the user name and password, other personal data is often used on the website for registration (e.g. full name, sex, country, town/city, phone number, email address, etc.). Password Manager can store this data in an encrypted Password Database in the form of Identities. To separate private and business information, you can create several Identities (see page 220). When you register in the program / on the web site, Password Manager will automatically use the chosen card to fill in the registration form. Using Identities saves time completing identical registration forms.

During authorization in the application / on the web page, Password Manager automatically enters personal data only if the Password Database is unlocked.

An account can be used in the following ways:

- Launch application / web page. The authorization form will be filled automatically using data from the account.
- Use Password Manager pointer. To do this, move the mouse cursor over the application icon in the taskbar notification area, then activate the account by dragging the Password Manager pointer to the required application / browser window.
- Select the account from the list of frequently used accounts. To do this, open the context menu of Password Manager and under frequently used accounts, select the required record.
- Use context menu of Password Manager. To do so, open the Password Manager context menu and select the **Accounts** → **<Account name>** item.

To use an Identity, please do the following:

1. Click the Caption Button in the upper-right corner of the application / browser window.
2. In the menu that will open, select the **Identities** → **<Identity name>** item. Password Manager automatically fills in the registration fields on the web page using data from the Identity.

FINDING PASSWORDS

A search for personal data could be hindered in the following cases:

- Some passwords are not associated with applications / websites.
- Password Database contains a large number of accounts.

Password Manager quickly finds passwords by the following parameters:

- account name;
- user name;
- key words (see page 216) (key word search parameters are set additionally for each user name);
- web address (for web addresses).

The search is performed both by full name, and by initial letters and any characters included in the account name or link.

To find an account / password, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. Enter the text in the **Password Manager** window that will open, in the search field.

   To view the data of the account for which the password is entered, press the **ENTER** key.

DELETING PERSONAL DATA

Before making any changes to personal data, Password Manager automatically creates a backup copy of the Password Database. If this data is accidentally changed or deleted, use Restore Password Database (see page 224). From the Password Database it is possible to delete one or all elements.

To delete an element from the Password Database, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window, under the tab **Edit**, select the element from the **My Passwords** list and click **Delete** or press **DEL** on the keyboard.

To delete all elements from the Password Database, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window, under the tab **Edit,** click **Delete all**.

IMPORTING / EXPORTING PASSWORDS

Password Manager is able to import and export your passwords.

The application allows passwords to be added from unprotected (unencrypted) password databases. You can import both passwords from other password management applications (e.g. Internet Explorer, Mozilla Firefox, KeePass passwords), and passwords that you have already exported from Password Manager. Passwords are imported from *.xml and *.ini files.

Password Manager can export the Password Database to *.xml, *.html or *.txt files. Export is convenient for opening general access passwords, printing the Password Database, or saving a backup copy of the Password Database to a file in a different format to Password Manager.

Exported passwords are stored in unencrypted files and are not protected from unauthorized access. Therefore, it is recommended to consider ways of protecting exported files in advance.

When imported, the Password Database is modified. You can choose one of the following actions to be performed on the Password Database:

- **Overwrite**. The current Password Database will be replaced with the imported one (all passwords stored in Password Manager's Password Database before import will be deleted).
- **Merge**. The Password Database will be supplemented with passwords imported from unprotected password databases. When merging, you are given the option of importing accounts into Password Manager.
- **Cancel**. The operation to import passwords will be cancelled.

To replace the current Password Database with a Password Database imported from another application, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Import** button.
3. In the **Import passwords** window, select the application from which passwords should be imported, and then click **Load passwords**.
4. In the **Password Manager File** window, select the file with passwords that you want to import and click **Open**. To cancel the selection, click **Cancel**.

5. In the window that will open, click the **Overwrite** button.

To merge the current Password Database with a Password Database imported from another application, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Import** button.
3. In the **Import Passwords** window, select the application from which passwords will be imported and click **Load passwords**.
4. In the **Password Manager File** window, select the file with passwords that you want to import and click **Open**. To cancel the selection, click **Cancel**.
5. In the **Load Password Manager** window, click **Merge**.
6. In the **Import passwords** window, check the ☑ box next to the required accounts, and then click the **Import** button.

   To select all the accounts from the list, check the box ☑ next to the selected application.

To export Password Database, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Export to text file** button.
3. Confirm that you want to export the Password Database by clicking **OK**. To avoid confirming the export of the password database in the future, check the ☑ **Do not show this notification in future** box.
4. In the **Export Password Database to unprotected file** window that will open, specify the name, path, and format of the file.

PASSWORD DATABASE BACKUP / RESTORE

Before any changes are made to Password Database, a backup copy is automatically created. The path of the reserve copy is set by default, but you can change it (see page 231). It is useful to restore passwords in the following cases:

- if the most recent changes need to be cancelled;
- if the Password Database was overwritten or deleted;
- if the current Password Database is inaccessible / damaged after a hardware or system failure.

All data in the backup copy is stored in encrypted form. Password Manager registers all changes to the Password Database. In the application, backup copies are displayed in a list and sorted according to date, beginning with the most recent. For each backup copy, the following data is provided:

- location;
- date and time of creation;
- changes made relative to the previous version.

You can use backup copies to solve the following tasks:

- restore a Password Database from a backup copy;
- delete copies of a backup storage;

- change the location of backup copies (see page 231).

To restore the Password Database, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Restore** button.
3. In the **Restore** window that will open, select a backup copy from the list and click the **Restore** button.
4. In the window, confirm the restoration by clicking **OK**.

To remove unnecessary backup copies, please do the following:

1. In the context menu of the application, select **Password Manager**.
2. In the **Password Manager** window that will open, on the **Backup** tab, click the **Restore** button.
3. In the **Restore** window that will open, in the list of backup copies, select the versions of backup copies to delete. To select several versions, hold the **CTRL** key.
4. Click **Delete**.
5. Confirm deletion of the backup storage by clicking **OK**.

CONFIGURING APPLICATION SETTINGS

The application settings can only be configured if Password Database is unlocked (see page 214). When editing the settings, you can do the following:

- set the time when the application is launched (see page 236);
- enable notifications (see page 236);
- specify the user name (see page 227) that will be used by default when creating a new account;
- set the time when the password was stored in clipboard (see page 237);
- create a list of frequently used accounts (see page 227);
- create a list of ignored websites (see page 228) for which Password Manager functions are not used;
- create a list of trusted websites (see page 228) for which Password Manager will allow readdressing;
- specify a key combination to quickly launch Password Manager functions (see page 229);
- change the path for storing Password Database (see page 230), backup copies (see page 231);
- change data encryption method (see page 232);
- set automatic locking of Password Database (see page 233);
- change Master Password (see page 234);
- set Access to Password Database (see page 233);
- change the location of Caption Button, create a list of applications supporting Caption Button (see page 237);
- create a list of supported applications (see page 235).

To edit Password Manager settings, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the section to be edited.
4. In the right part of the window, enter the changes to the settings for the chosen section.

IN THIS SECTION:

DEFAULT USER NAME

Password Manager allows a user name to be set that will be automatically displayed in the **User name** field when creating a new account (see page 215).

To set the default user name, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the **Main settings** section.
4. In the right part of the window, fill in the **Default Login** field.

LIST OF FREQUENTLY USED ACCOUNTS

Password Manager provides quick access to accounts. The application menu can display a list of frequently used accounts. It shows the names of applications / web pages that you use most frequently. Items in the list are arranged in alphabetical order or by frequency of use.

The list of frequently used accounts is available in the menu if Password Database is not locked (see page 214).

You can set the following list options:

- **Number of items in the list** – maximum number of frequently used accounts that are displayed in the context menu of the application;
- **Display list in application menu** – the list of frequently used accounts will be accessible in the context menu of Password Manager;
- **Display in the Caption Button menu** – the list of frequently used accounts will be accessible in the Caption Button menu (from the application / browser window).

To display frequently used accounts in the menu, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Frequently used accounts**.
4. In the right part of the window, check the box **Show the list in the system tray menu**.

   To display the list of frequently used accounts in the Caption Button menu, additionally select the **Display in the Caption Button menu** checkbox.

   If the **Show the list in the system tray menu** checkbox is not enabled, the remaining options in the list cannot be modified.
5. Specify the number of accounts in the **List size** field.
6. If necessary, modify the items in the list manually. To remove an item from the list, select the required account in it, and click **Delete**. To delete all items from the list, click **Clear**.

LIST OF IGNORED WEB ADDRESSES

Password Manager usually offers to add a new account at the first authorization at a website. In this case, the personal data will be automatically re-entered at each next visit of this website.

To enter your personal data on your own at each next authorization, you can configure a list of web addresses that will not be covered by Password Manager functions. Automatic input of user name and password is disabled for websites on this list. Besides, Password Manager will automatically abstain from offering you to create a new account (see page 215)/ user name (see page 219).

To create a list of ignored web addresses, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the **Ignored web addresses** section.
4. In the right part of the window, click **Add**, enter the web address and press **ENTER**.

   To change a web address, select it from the list and click **Edit**. To delete a web address from the list, select it and click **Delete**.

LIST OF TRUSTED WEB ADDRESSES

Password Manager protects your personal data from phishing attacks. If during authorization you were redirected to another website, the application will notify you about it.

Phishers often use redirecting to websites that give access to bank accounts (e.g. Internet banking sites, payment systems, etc.). On the company's official authorization page, users are redirected to a counterfeit website visually similar to the official page. All data entered on the counterfeit page falls into the hands of attackers.

Redirecting is often officially installed on websites. If you don't want Password Manager to consider readdressing to be a phishing attack, you can create a list of trusted web addresses. The list of trusted web addresses includes websites to which the entered personal data are transferred. During authorization, Password Manager will not notify you of the personal data being transferred to a trusted website.

Password Manager allows transferring personal data to trusted websites from other websites. Before adding a website to the list of trusted web addresses, make sure it is completely reliable!

You can add a website to the list of trusted web addresses in the following ways:

- directly during authorization on the website;
- manually, from the **Password Manager Configuration** window.

To add a website to the list of trusted web addresses during authorization on the website, wait to be redirected from one website to the other, and then, in the Password Manager window, select the check box **Always trust <name of website>**.

To create a list of trusted web addresses manually, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part **Settings** window, select **Trusted web addresses**.
4. In the right part of the window, click **Add**. The field in the **Trusted web addresses** list will become active. Then, enter the web address and press **ENTER**.

   To change the web address, select it in the list and click **Edit**. To delete the web address from the list, select it in the list and click **Delete**.

QUICK LAUNCH OF APPLICATION FUNCTIONS

To quickly access certain application functions, it is convenient to use hotkeys.

You can specify hotkeys for the following actions:

- Lock / Unlock Password Manager (see page 214).
- Enter the password.
- Show virtual keyboard.

To access functions quickly, you can specify one key or a combination of two or three keys.

Avoid key combinations used by Microsoft Windows to access functions.

To change a key combination, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Hot keys**.

4. In the right part of the window, set the required key combination for each action.

PASSWORD DATABASE LOCATION

Password Manager's Password Database is an encrypted file (see page 232) that stores all your personal data (accounts, user names, passwords, and Identities).

To use the Password Database, you need to unlock it (see page 214) (get authorized). By default, access to personal data is protected by the Master Password. Additionally, Password Manager secures the Password Database using USB or Bluetooth devices. You can change the access parameters (see page 233) for each Password Database.

The default paths for different versions of Microsoft Windows are as follows:

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

You can use different media to store your Password Database: removable disk, local disk, or network drive.

The following actions are possible when changing the path or names of the Password Database:

- **Copy** – creates a copy of the Password Database with the specified path. This copy will become an active Password Database.
- **Move** – the active Password Database will be saved with the specified path.
- **Create new Password Database** – creates an empty copy of the Password Database that will become active.

To move or rename the Password Database, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **My Passwords**.
4. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
5. In the **Select Password Database** window, specify the name and path of the file and click the **Open** button.
6. In the **Password Database location** window, select the required action to be performed on the Password Database and confirm it by clicking **OK**.
7. In the **Password Manager** window, enter the Master Password to confirm the changes.

To change the current Password Database, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **My Passwords**.
4. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
5. In the **Select Password Database** window, select the Password Database file and click the **Open** button.
6. In the **Password Manager** window, enter the Master Password of the restored Password Database.

CREATING NEW PASSWORD DATABASE

Password Manager allows the use of several Password Databases. Creating a new Password Database allows your personal data to be separated and saved in two or more Password Databases. If necessary, an old Password Database can be restored. Password Manager can create a new Password Database if the current Password Database is damaged or cannot be restored from a backup copy.

To create a new Password Database, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **My Passwords**.
4. In the right part of the window under **Location**, click  located in the right part of the **Path** field.
5. In the **Select Password Database** window, specify the location and filename of the Password Database and click **Open**.
6. In the **Password Database location**, select the **Create new Password Database** action and click **OK**.
7. In the **New Password Database** window, under **Password**, set the password for access to the new database and re-enter it in the field **Confirm password**.

   If the password is re-entered incorrectly, it will be highlighted red.

   Under **Encryption algorithm** select the encryption provider and required encryption method (see page 232).
8. In the displayed window, enter the new Master Password to confirm creation of a new Password Database.

PASSWORD DATABASE BACKUP

Before saving any changes to your personal data, Password Manager automatically makes backup copies of the Password Database. This avoids any losses of data in the event of system or technical failure. Password Manager creates a complete copy of the Password Database before implementing the changes. If the Password Database is damaged, you can restore data from the most recent backup copy of the Password Database (see page 224).

You can use different media to store the backup copy of your Password Database: local disk, removable disk, or network drive.

By default, depending on the operating system, the backup copy is saved with the following path:

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

To change the path of the backup file, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **My Passwords**.

4. In the right part of the window, under **Backup**, click the button  located in the right part of the field **Path**.

5. In the **Browse For Folder** window, select the folder for the backup copy of the Password Database.

SELECTING ENCRYPTION METHOD

The task of cryptography is to protect information from unauthorized access and distribution. The main purpose of the cipher is to transfer encrypted messages via unprotected channels.

Keys are required for encryption and decryption. A key is a vital component of a cipher. If one and the same key is used for encryption and decryption, it is called a symmetric key. If two keys are used , it is asymmetric. Symmetric ciphers can be either block or stream. Any information (regardless of the format of the source data) is interpreted in binary code. A block cipher assumes all data will be broken into blocks, each of which will then undergo an independent transformation. In a stream cipher, the algorithm is applied to each bit of information.

Password Manager offers the following symmetric algorithms:

- **DES**. Block cipher with the standard-sized key of 56 bit. By today's standards, DES does not offer a high level of protection. This algorithm is used when reliability is not the main requirement.

- **3DES**. A block algorithm created based on DES. It solves the main weakness of its predecessor – the small key size. 3DES keys are three times the size of those used by DES (56*3=168 bits). The speed of operation is three times slower than for DES, but the level of security is much higher. 3DES is used more often, since DES is not resilient enough against modern cracking techniques.

- **3DES TWO KEY**. A block algorithm created based on DES. This is a 3DES algorithm which uses a key size of 112 bits (56*2).

- **RC2**. A block-cipher algorithm with variable-length key quickly processes a large amount of information. It is a faster algorithm than DES. In terms of security and resilience, it is comparable to 3DES.

- **RC4**. A stream cipher with variable-length key. The key size can range from 40 to 256 bits. The advantages of the algorithm are its high speed and variable key size. By default, Password Manager uses RC4 to encrypt data.

- **AES**. A block-cipher symmetric algorithm with a key length of 128, 192, 256 bits. This algorithm guarantees a high level of security and is one of the most commonly used.

Microsoft Windows uses an encryption provider to perform cryptographic operations. Each encryption provider supports several encryption algorithms with a specified key length. Password Manager uses the following built-in Microsoft Windows encryption providers:

- Microsoft Base Cryptographic Provider;

- Microsoft Enhanced Cryptographic Provider;

- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype);

- Microsoft RSA/Schannel Cryptographic Provider;

- Microsoft Strong Cryptographic Provider.

To change the encryption algorithm, please do the following:

1. Open the main application window.

2. In the **Security+** section, click **Password Manager**.

3. In the left part of the **Settings** window, select **My Passwords**.

4. In the right part of the window, under **My Encryption**, click **Change**.

5. In the **Encryption algorithm** window, specify the parameters of the encryption algorithm.

AUTOMATIC LOCKING OF PASSWORD DATABASE

Password Manager automatically locks the Password Database after launching an application and after a specified time during which the computer was not used. You can specify the time interval after which the Password Database will be locked. The value of the interval varies from 1 to 60 minutes. It is recommended that the Password Database be locked after 5-20 minutes of computer inactivity. You can also disable the automatic blocking of Password Database.

Password Manager automatically locks the Password Database after a set period of computer inactivity. If automatic locking of the computer is disabled, your personal data will not be protected if you leave your computer without locking it manually.

To modify the interval after which the Password Database becomes locked, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **My Passwords**.
4. In the right part of the window, under **Automatic locking**, use the drop-down list to select the time after which Password Manager will be locked.

   To disable the locking of Password Database, select **Never**.

PASSWORD MANAGER AUTHORIZATION METHOD

Authorization enables to control access to your personal data. You can use one of the following authorization methods:

- **Master Password**. To unlock the Password Database, you must enter the Master Password. This is the default authorization method.
- **USB device**. To access the Password Database, connect any USB device to your computer. For example, flash cards, cameras, MP3 players, and external hard drives can be used as a USB device. When the USB device is disabled, the Password Database is automatically locked.
- **Bluetooth device**. To access the Password Database, use a Bluetooth device. Bluetooth must be enabled on both the mobile phone and the computer which uses Password Manager. When connecting a mobile phone and computer via Bluetooth, the Password Database will be unlocked. If the link drops (e.g. you disable Bluetooth on the mobile phone), the Password Database will be locked.
- **No authorization**. Access to the database is unprotected.

  Without authorization, your personal data is accessible to all users who work on your computer.

If you select authorization using a USB or Bluetooth device, you are recommended to remember your Master Password. If there is no authorization device available, Password Manager enables the use of Master Password for access to your personal data.

To change the authorization method, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Authorization method**.

4. In the right part of the window, under **Authorization method**, select an authorization option from the drop-down list.

SEE ALSO:

USING USB AND BLUETOOTH DEVICES

To access the Password Database (see page 233), Password Manager allows the use of various USB and Bluetooth devices.

To use a USB device to access the Password Database, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Authorization method**.
4. In the right part of the window, under **Authorization method**, select the **USB device** value from the drop-down list.
5. Connect the removable device to the computer.
6. Select a device from the **Disk drives** list and click **Set**. The icon appears next to the chosen device. If the connected device does not appear in the list, check the **Show additional devices** box. If necessary, you can change the authorization device by clicking **Reset**.

To use a Bluetooth device to access the Password Database, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Authorization method**.
4. In the right part of the window under **Authorization method**, select the value **Bluetooth device** from the drop-down list.
5. Enable Bluetooth on your computer, and then on the device.
6. Select a device from the **Phones and modems** list, and then click **Set**. The icon appears next to the chosen device. If necessary, you can change the authorization device by clicking **Reset**.

CHANGING MASTER PASSWORD

Password Manager allows the Master Password to be used to access your Password Database (see page 233). Thus, you only need to remember one password. By default, a Master Password is created when Password Manager is launched for the first time. You can change it later. The security of your personal data depends to a great extent on the reliability of Master Password. When creating a Master Password, Password Manager automatically evaluates its strength and assigns it a particular status:

- low strength;
- normal;

- high.

To create a secure password, use special symbols, numbers, upper- and lower-case letters. It is not recommended to use information that can be easily guessed (e.g. family members' names or dates of birth) as a password.

When changing the Master Password, Password Manager requests confirmation of the input password (the new password should be entered again). The new password cannot be saved without confirmation. If the confirmation password does not match the entered password, the confirmed password will be highlighted red. In this case, a warning message will appear when you try to save the new password.

To change the Master Password, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Authorization method**.
4. In the right part of the window, under **Password protection**, click **Change**.
5. In the **Password protection** window, enter the new password, then confirm it by reentering it in the **Confirm password** field.

CREATING A LIST OF SUPPORTED BROWSERS

To ensure that automatic activation of the account and the Caption Button (see page 237) are working correctly, for several browsers and mail clients Password Manager requests the installation of additional expansion modules (plug-ins). By default, plug-ins are installed when Password Manager is first launched. You can install additional plug-ins.

Password Manager contains a list of web browsers and mail clients where each program is assigned the status, **Installed** or **Not installed** depending on whether the required plug-in is installed, or not.

It is recommended to close all programs for which the plug-in will be installed.

To install a plug-in for a browser or mail client, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Supported browsers**.
4. In the right part of the window, select a program from the list of **Supported browsers and available extensions**, then click **Install**.
5. Follow the instructions in the **Installation wizard**. When the plug-in is installed, the program will automatically move to the group **Installed**. It will be assigned the status **Installed**. You can delete an installed plug-in by clicking **Uninstall**.

ADDITIONAL SETTINGS

You can configure the following additional settings for Password Manager:

- the time when the application is launched (see page 236);
- action launched by double-clicking (see page 236);
- receipt of notifications (see page 236);

- the time when the password was stored in clipboard (see page 237);
- Caption Button (see page 237).

APPLICATION LAUNCH TIME

By default, Password Manager loads automatically when the operating system starts up. You can change the application's start-up parameters.

To launch the application manually, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the **Main settings** section.
4. In the right part of the window, in the **Main settings** block, uncheck the **Launch Password Manager at computer startup** box.

DOUBLE-CLICK ACTION

Password Manager can set a task to be launched by double-clicking the application icon the taskbar notification area of Microsoft Windows. One of the following tasks can be launched in this way:

- open the main Password Manager window (see page 212);
- lock / unlock Password Manager (default action).

To set the task to be launched by double-clicking the application icon in the taskbar notification area, please do the following:

1. Open the main applicationwindow.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the **Main settings** section.
4. In the right part of the window, select the action from the drop-down list **On double-click**.

NOTIFICATIONS

When Password Manager is running, various events occur that are of an informational nature. To keep up to date, use the notifications service. Users are notified of events by prompts and pop-up messages.

The following types of notifications are implemented in the application:

- **Application start**. A message appears upon application restart, when the application has already been started and the Password Database is not locked.
- **Account activation**. A message appears when the account is activated.
- **Clear clipboard**. Password Manager can temporarily store the password in clipboard. This is convenient when data needs to be copied and then pasted in the selected field. When the specified time expires (see page 237), the password will be deleted from clipboard.
- **Automatically block Password Manager**. The message appears when Password Manager automatically blocks the password database. By default, Password Manager automatically locks the Password Database after the operating system starts up and after a specified time (see page 233), during which the computer is not used.

- **Exporting passwords to unencrypted file**. A warning message saying that after export, your passwords will be saved in a non-encrypted file, and will consequently be made accessible to any user working on your computer. We recommend that before exporting data you consider ways of protecting the file containing passwords.

- **Manual form edit**. To set parameters for additional fields, the application requests permission to use the default browser. The message warns that images and system files (cookies) will be saved on your computer.

- **Warn about difficulties populating login information for the Account**. This message warns that personal data cannot be entered automatically during authorization.

To receive notifications, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the **Main settings** section.
4. In the right part of the window, click the **Notification settings** button in the **Main settings** block.
5. In the displayed window, check or uncheck the box next to the required types of notifications.

BACKUP TIME OF PASSWORD IN CLIPBOARD

Password Manager can copy the password to the clipboard for a specified period of time. This is convenient for quick actions with passwords (e.g. when you need to use a created password to register on a website / in an application). You can set the amount of time the password will be saved in the clipboard. When this time expires, the password is automatically deleted from the clipboard. This will prevent the interception and theft of passwords because they will not be able to be copied from the clipboard when the specified time expires.

To change the backup time of the password in the clipboard, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select the **Main settings** section.
4. In the right part of the window, under **Clipboard**, set the time in seconds.

CAPTION BUTTON

Password Manager can manage accounts directly from the application / browser window via the Caption Button located in the upper-right corner of the application / browser window. Clicking the Caption Button opens a menu with a list of user names that are related to the application / web page. When selecting a user name, Password Manager automatically fills in authorization fields using data from the Password Database.

The Caption Button is accessible if the Password Database is not locked (see page 214).

If, in addition to the Program Manager menu, the application you are working with has other embedded application menus, you can set the position of the Caption Button in relation to the other buttons. Besides, it is possible to generate a list of browsers for which the Caption Button is used.

To change the Caption Button parameters, please do the following:

1. Open the main application window.
2. In the **Security+** section, click **Password Manager**.
3. In the left part of the **Settings** window, select **Caption Button**.

4. In the right part of the window, under **Caption Button display**, set the required parameters in accordance with the task:

   - To change the location of the Caption Button, under **Caption Button display**, enter the position number of the button (how many buttons will be located to the right of the Caption Button).

   - To prevent the Caption Button from being displayed when locking the Password Database, in the **Display Caption Button** block, check the  **Do not display button if Password Manager is locked** box.

   - To create a list of browsers in which the Caption Button is available, under **Caption Button in web browsers**, check the box  next to the required browser from the list.

ADDITIONAL FEATURES

My Password Manager includes a number of other tools:

- **Password generator** can create secure passwords for accounts.
- The **Password Manager pointer** can quickly select an application / web page and then automatically define the action for the chosen object.

IN THIS SECTION:

PASSWORD GENERATOR

Data security depends directly on the strength of the passwords. Data could be at risk in the following cases:

- one password is used for all accounts;
- the password is simple;
- the password uses information that is easy to guess (e.g. family members' names or dates of birth).

To ensure data security, Password Manager allows unique and reliable passwords to be created for accounts. Password Manager saves all generated passwords, which means they do not need to be remembered.

A password is considered secure if it consists of more than four characters and contains special symbols, numbers, and upper- and lower-case letters.

Password security is determined by the following parameters:

- **Length** – the number of symbols in the password. This value can range from 4 to 99 symbols. The longer the password, the more secure it is considered to be.
- **A-Z** – uppercase letters.
- **a-z** – lowercase letters.
- **0-9** – numbers.
- **Special symbols** – special symbols.
- **Exclude similar symbols** – the use of identical symbols in a password is not permitted.

Password generator can be used in solving the following tasks:

- when creating a new account in an application / on a website;
- when adding an account (see page 215) / user name (see page 219) in Password Manager manually.

➡ *To use Password generator when creating a new account in an application / on a website, please do the following:*

1. Open the context menu of Password Manager and select **Password Generator**.

2. In the **Password generator** window, specify the number of symbols in the password in the **Password length** field.

3. If necessary, you can specify additional settings for Password generator under **Additional** by checking / unchecking the box next to the required settings.

4. Click **Generate**. The generated password is displayed in the **Password** field. To view the generated password, check the box **Show password**.

5. Paste the password to clipboard by using the button , then enter the password in the password input field in the application / on the web page by pressing **CTRL+V**. The generated password is stored in clipboard for a specified period of time before being deleted.

6. Check the box **By default** to save the specified settings.

PASSWORD MANAGER POINTER

Password Manager makes it easy to use your accounts. Password Manager pointer allows you to quickly select the application / web page for which you want to enter personal data.

When launching the application / web page, Password Manager automatically looks for a sticky account in the Password Database. If an account is found, the personal data is entered in the authorization fields automatically. If there is no sticky account in the Password Database, Password Manager provides the option to add a new account. In the application / browser window, a search is automatically performed for fields containing the user name and password. In the displayed application / browser window, the fields are automatically filled using data found in the Password Database. You only need to fill in the empty fields.

To use the Password Manager pointer, please do the following:

1. Point the mouse cursor on the Password Manager icon the taskbar notification area and wait a few seconds.

2. When it appears, drag the Password Manager pointer to the required application / browser window. Password Manager automatically defines the action to be performed on the chosen application / web page.

MY CONTROL CENTER

Control Center is designed for remote control of Kaspersky PURE installed on networked computers. The control is performed from the administrator's workstation.

The network administrator can take the following actions via Control Center:

- analysis of protection level of networked computers;
- scan of the whole network or individual computers for threats;
- centralized update of anti-virus databases;
- modification of the protection settings for networked computers;
- Parental Control;
- data backup on networked computers;
- viewing of reports on security subsystems' operation.

To launch My Control Center, please do the following:

In the top part of the Kaspersky PURE main window, click the **My Control Center** link.

At the first startup, the Remote Control Configuration Wizard starts automatically (see section "Configuring remote management" on page 241). At further startups, you will need to enter the password.

For remote management via local network, the Control Center password should be identical on all computers.

IN THIS SECTION:

CONFIGURING REMOTE MANAGEMENT

Remote control is configured using the wizard. At the first startup of Control Center, the Configuration Wizard starts automatically.

This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You can also switch between the wizard's steps that you have completed, by using the browsing buttons in the top part of the window.

To configure the Control Center, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. The Remote Control Configuration Wizard will be started. At the first startup of Control Center, the Configuration Wizard starts automatically. Let us take a closer look at the wizard's steps:
   a. Enter or set the administrator password in the **Password protection** window.
   b. Select a network subject to remote control in the **Network scan** window.
   c. Select the update mode for anti-virus databases in the **Update source** window.
   d. Confirm the settings you have selected in the **Summary** window.

ANALYZING NETWORK SECURITY

The top part of My Control Center window displays the current status of the network protection.

There are three possible values of protection status: each of them is indicated with a certain color, similar to traffic lights. Green indicates that your network's protection is at the proper level, while yellow and red colors indicate that there are various security threats. In addition to malicious programs, threats include obsolete application databases, disabled protection components, the selection of minimum protection settings etc. Security threats must be eliminated as they appear.

To obtain detailed information about problems in the network protection and eliminate them, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, click the status icon or the icon of the panel on which it is located (see fig. above).

   In the **Network protection state** window that will open, current problems are displayed.

Also, you can view the list of problems on an individual networked computer and eliminate some of them remotely.

To obtain the list of problems on an individual networked computer, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select the computer for which you want to view the list of problems, and go to the **Information** section.
3. In the right part of the window that will open, select the **Problems list** item.

   In the **Protection state** window that will open, current problems encountered on the selected computer are displayed.

MANAGING PROTECTION COMPONENTS

Using Control Center, you can remotely turn on / off different protection components on the networked computers.

To turn on / off a protection component remotely, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select the computer for which protection management is required, and go to the **Information** section.
3. In the right part of the window, select the **Protection components status** item.
4. In the window that opens, enable / disable the required protection component by clicking its name.

MANAGING LICENSES

Using Control Center, you can remotely check the license status on the networked computers, renew the license, or activate a new one.

To manage the license on a networked computer, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select the computer for which you want to view the list of problems, and go to the **Information** section.
3. In the right part of the window that will open, select the **License manager** item.
4. In the **License manager** window that will open, take the required actions.

PARENTAL CONTROL MANAGEMENT

Using the Control Center, you can remotely set restrictions and view the statistics of events related to the users' activities on the networked computers and on the Internet, or related to the instant messaging.

To configure Parental Control, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select a computer in the top part of the window and go to the **Parental Control** section.
3. In the right part of the window, select an account and click the **Configure** button.

To view the statistics, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select a computer in the top part of the window and go to the **Parental Control** section.
3. In the right part of the window, select an account and click the **Detailed report** button.

REMOTE SCAN FOR VIRUSES AND VULNERABILITIES

Using the Control Center, you can run a virus scan task remotely either for the whole network, or for an individual computer.

To scan the whole network for viruses, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, click the **Perform virus scan** link in the **Actions for network** block in the top part of the window.
3. In the **Group start of scan** window that will open, select the scan type and the computers you need to scan.

To scan an individual computer for viruses or vulnerabilities, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select a computer in the top part of the window and go to the **Scan** section.
3. In the right part of the window, select the required scan task.

UPDATING DATABASES AND APPLICATION MODULES

Using the Control Center, you can remotely manage the updating of Kaspersky PURE on the networked computers.

You can select one of the following update modes:

- Independent update of the databases on the computers.
- Centralized update via a dedicated update server.

To change the update mode for the networked computers, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, click the **Settings** link in the top part of the window.
3. In the Control Center Configuration Wizard that opens, proceed to the **Update server** step and select the required update mode.

When the centralized update is selected, one of the networked computers should be the update server. Other computers download updates from the server you have selected.

To select the update server, please do the following:

1. Open the main applicationwindow and click the **Control Center** link in the top part of the window.
2. In the top part of the window that will open, select a computer and go to the **Update** section.
3. Click the **Select as the update server** button.

You can run an update task remotely either for the whole network, or for an individual computer.

To run update on all the networked computers, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the top part of the window that will open, click the **Perform update** link in the **Actions for network** menu.

3. In the **Group start of update** window that will open, select the computers on which you need to download the updates.

To run the update on an individual computer, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the top part of the window that will open, select a computer and go to the **Update** section.
3. In the right part of the window, click the **Perform update** button.

REMOTE BACKUP

Using the Control Center, you can remotely run backup tasks on the networked computers, as well as view the report on executed backup tasks and data restoration tasks.

To backup objects remotely, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select a computer in the top part of the window and go to the **Backup** section.
3. In the right part of the window, select a backup task and click the **Run** button.

   You can pause or stop the task execution, by using the corresponding buttons in the top part of the window.

To obtain a report on the execution of backup tasks and data restoration tasks, please do the following:

1. Open the main application window and click the **Control Center** link in the top part of the window.
2. In the window that will open, select a computer in the top part of the window and go to the **Backup** section.
3. Click the **View report** button in the top part of the window.
4. In the **Report** window that will open, specify the event display settings.

CONFIGURING KASPERSKY PURE SETTINGS

The application settings window is used for quick access to the main Kaspersky PURE settings.

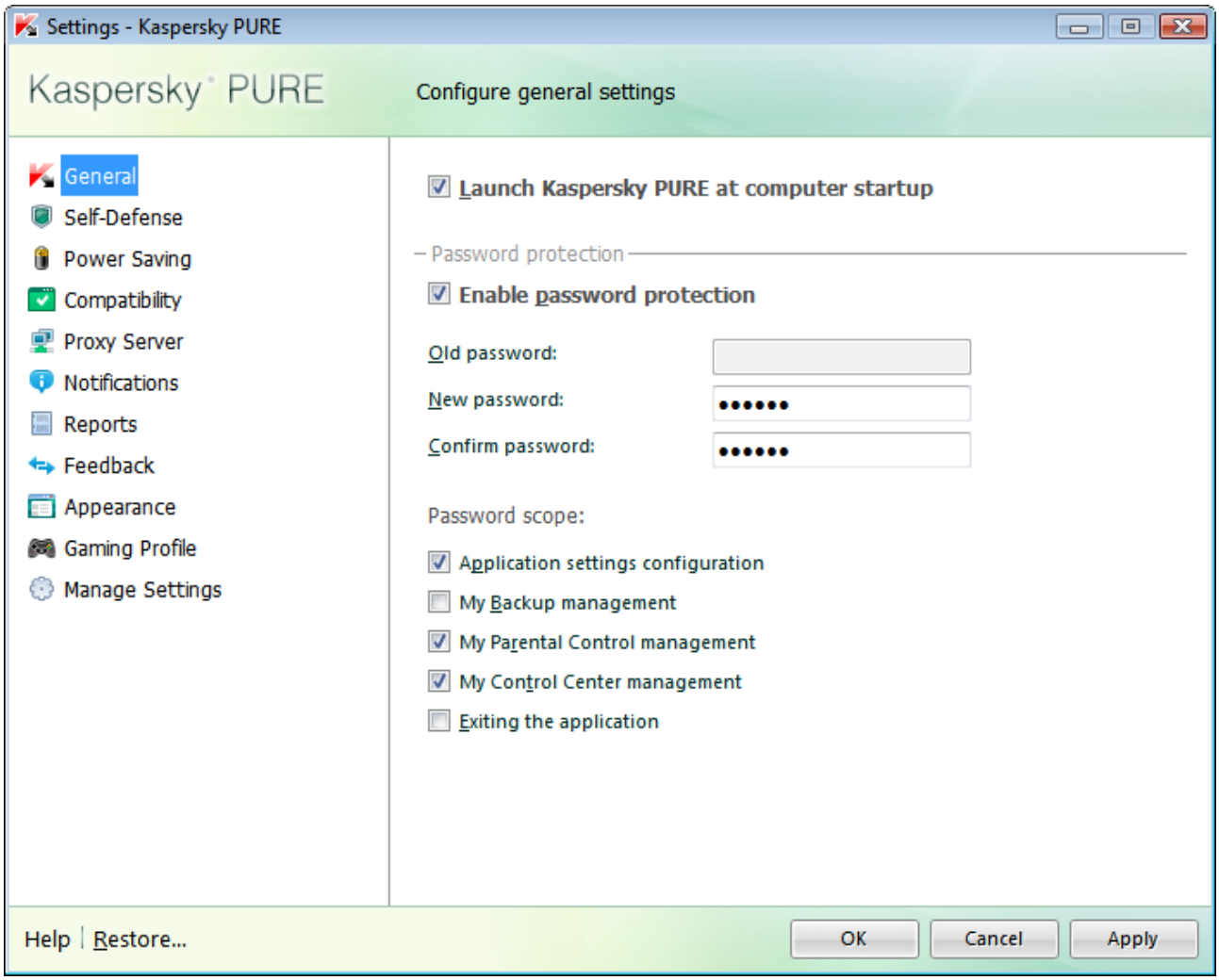


Figure 23. Configuring Kaspersky Anti-Virus

The application settings window consists of two parts:

- the left part of the window provides access to Kaspersky PURE settings, virus scan tasks, update tasks, etc.;
- the right part of the window contains a list of parameters for the setting, task, etc., selected in the left part of the window.

You can open this window:

- From the main application window (see page 51). To do so, click the **Settings** link in the top part of the main window.

- From the context menu (see page. 50). To do so, select the **Settings** item from the application context menu.

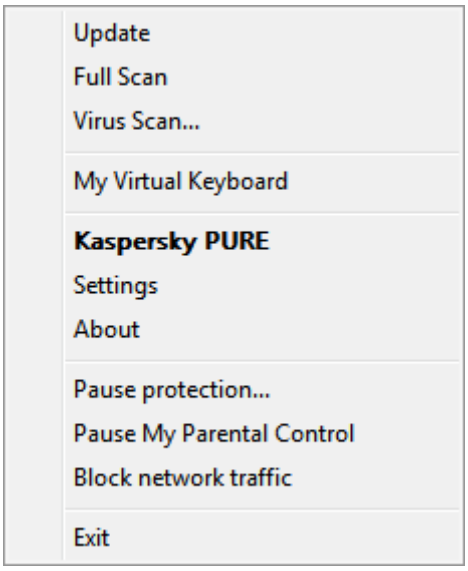


Figure 24. Context menu

IN THIS SECTION:

GENERAL SETTINGS

In this window, you can use the following advanced functions of Kaspersky PURE:

- Running Kaspersky PURE at system startup (see page 248).
- Restricting access to Kaspersky PURE (see page 248).

RUNNING KASPERSKY PURE AT WINDOWS STARTUP

If you have to completely shut down Kaspersky PURE for any reason, select the **Exit** item from the Kaspersky PURE context menu. As a result, the application will unload from RAM. This means that your computer will be running unprotected.

You can re-enable the computer's protection by loading Kaspersky PURE from the **Start** → **Programs** → **Kaspersky PURE** → **Kaspersky PURE** menu.

Protection can also be resumed automatically after restarting your operating system.

To enable this mode:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that opens, select the **General** section and check the **Launch Kaspersky PURE at computer startup** box.

RESTRICTING ACCESS TO KASPERSKY PURE

A personal computer may be used by several users, including those with different level of computer literacy. Leaving open access to Kaspersky PURE and its settings may dramatically lower the computer's security level as a whole.

To increase the security level of your computer, use a password to access Kaspersky PURE. You can block any Kaspersky PURE's operations, except for notifications of dangerous objects detection, or prevent the following actions from being performed:

- changing application settings;
- backup management;
- parental control management;
- remote management of network security;
- closing the application.

To protect access to Kaspersky PURE with a password, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that will open, select the **General** section, and under **Password protection** check the **Enable password protection** box and click the **Settings** button.
3. In the **Password protection** window that will open, enter the password and specify the scope to be covered by the access restriction. Now whenever any user on your computer attempts to perform the actions you have selected, Kaspersky PURE will always request the password.

SELF-DEFENSE

Kaspersky PURE ensures your computer’s security against malware and, because of that, can be the target of malicious programs which may try to block or even delete it.

To ensure the reliability of your computer's security system, Kaspersky PURE is provided with features of self-defense and protection against remote access.

On computers running under 64-bit operating systems and Microsoft Windows Vista, self-defense is only available to prevent changing or deleting Kaspersky PURE's own files on local drives and system registry records.

Frequent are the situations when remote administration programs (such as RemoteAdmin) are needed while using the remote access protection. To ensure their normal performance, you should add these programs to the list of trusted applications and enable the **Do not monitor application activity** option for them.

To enable Kaspersky PURE's self-defense mechanisms, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, select the **Self-Defense** section. In the **Self-Defense** section, check the **Enable Self-Defense** box to activate the Kaspersky PURE's mechanism of protection of files on the disk, memory processes and system registry records from being modified or deleted.

   In the **Self-defense** section, check the **Disable external service control** box to block any attempt to remotely manage the application's services.

   If any of the actions listed are attempted, a message will appear over the application icon in the taskbar notification area (unless the notification service has been disabled by the user).

BATTERY SAVING

To save power on a portable computer, virus scan tasks may be postponed.

Since both scanning for viruses and updating often require significant resources and time, you are advised to disable the scheduled startup of those tasks. This will allow you to save the battery charge. If necessary, you can update Kaspersky PURE or start a virus scan on your own.

To use the battery saving service, please do the following:

1. Open the main application window and click the **Settings** link in the top part.

2. In the window that will open, select the **Battery saving** section and check the **Disable scheduled scans while running on battery power** box.

COMPATIBILITY

In this window, you can use the following advanced functions of Kaspersky PURE:

- Using advanced disinfection technology (see page 249).
- Postponing the virus scan task execution when it slows down other applications (see page 250).

ADVANCED DISINFECTION TECHNOLOGY

Today's malicious programs can invade the lowest levels of an operating system which makes them practically impossible to delete. If a malicious activity is detected within the system, Kaspersky PURE will offer you to perform a special advanced disinfection procedure which will allow to eliminate the threat and delete it from the computer.

After this procedure, you will need to restart your computer. After restarting your computer, you are advised to run the full virus scan.

To start the advanced disinfection procedure, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, select the **Compatibility** section and check the **Enable advanced disinfection technology** box.

COMPUTER PERFORMANCE DURING TASK EXECUTION

Virus scan tasks may be postponed to limit the load on the central processing unit (CPU) and disk storage subsystems.

Executing scan tasks increases the load on the CPU and disk subsystems, thus slowing down other applications. By default, if such a situation arises, Kaspersky PURE will pause virus scan tasks and release system resources for the user's applications.

However, there is a number of applications which will start immediately when CPU resources become available, and will run in the background. For the scan not to depend on the performance of those applications, system resources should not be conceded to them.

Note that this setting can be configured individually for every scan task. In this case, the configuration for a specific task has a higher priority.

In order to postpone the execution of scan tasks if it slows down other programs:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, select the **Compatibility** section and check the **Concede resources to other applications** box.

PROXY SERVER

If the computer's Internet connection is made through a proxy server, you may need to edit its connection settings. Kaspersky PURE uses those settings for certain protection components, and for updating databases and application modules.

If your network includes a proxy server using a nonstandard port, you should add the port number to the list of monitored ports (see section "Creating a list of monitored ports" on page 169).

To configure the proxy server, please do the following:

1. Open the main application window and click the **Settings** link in the top part.

2. In the window that will open, select the **Proxy Server** section and configure the connection settings.

NOTIFICATIONS

During Kaspersky PURE's operation, various events may occur. They may be of informative character or contain important information. For example, an event can inform you of a successful completion of an application update, or can record an error in the operation of a certain component that should be immediately eliminated.

To keep up with the events in Kaspersky PURE's operation, use the notification service.

By default, the user is notified of the events by pop-up messages with an audio signal.

Notifications can be delivered in one of the following ways:

- Pop-up messages appearing over the application icon in the system tray;
- Audio messages;

- Email messages.

To disable notification delivery, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Notifications** section and uncheck the **Enable events notifications** box.

Even if the notification delivery is disabled, information about events occurring in Kaspersky PURE's operation will be recorded in the report on the application's operation.

To select the notification delivery method, please do the following:

1. Openthe main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Notifications** section and click the **Settings** button.
3. In the **Notifications** window that will open, select the notification delivery method.

SEE ALSO:

DISABLING SOUND NOTIFICATIONS

By default, all notifications are accompanied by an audio signal; Microsoft Windows sound scheme is used for this purpose. The **Use Windows Default sound scheme** box allows to change the scheme being used. If the box is unchecked, the sound scheme from previous application versions will be used.

To disable sound notifications, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Notifications** section. In the **Audio messages** block, uncheck the **Enable sound notifications** box.

DELIVERY OF NOTIFICATIONS USING EMAIL

If notifications are to be delivered by email, edit the delivery settings.

To modify the email settings for notification delivering, please do the following:

1. Open the main application windowand click the Settings link in the top part of the window.
2. In the window that will open, select the **Notifications** section.
3. Check the **Enable email notifications** box and click the **Email settings** button.
4. In the **Email notification settings** window that will open, specify the delivery settings.

REPORTS

In this section, you can configure report creation (see page 252) and storage (see page 252).

LOGGING EVENTS INTO REPORT

You can add information about non-critical events, and registry and file system events to the report. By default, these events are not recorded in the report.

To add information about non-critical events, and registry and file system events to the report:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Reports** section and check the required box.

CLEARING THE APPLICATION REPORTS

Information about the Kaspersky PURE operation is logged in the reports. You can clear them.

To clear the reports*, please do the following*:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Reports** section and click the **Clear** button.
3. In the **Deleting information from reports** window that will open, check boxes for the report categories you want to clear.

STORING REPORTS

You can determine the maximum storage time for event reports (the **Store reports no longer than** box). By default, it is equal to 30 days: after it expires, objects will be deleted. You can change the maximum storage time, or even discard any limits imposed on it. Besides, you can specify the maximum size of report file (the **Maximum file size** box). By default, the maximum size is 1024 MB. Once the maximum size has been reached, the content of the file will be overwritten with new records. You can cancel any limits set on the report's size, or enter another value.

To configure the settings of report storage, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that will open, select the **Reports** section and check the required boxes. Change the maximum size of the report and its storage period, if necessary.

FEEDBACK

A great number of new threats appear worldwide on a daily basis. To facilitate gathering statistics about new threat types and sources, and about elimination methods, Kaspersky Lab invites you to use the *Kaspersky Security Network* service.

Using Kaspersky Security Network suggests sending certain information to Kaspersky Lab. The following data will be sent:

- Unique identifier assigned to your computer by the Kaspersky Lab's application. This identifier characterizes the hardware settings of your computer and contains no private information.

- Information about threats detected by application's components. The information's structure and contents depend on the type of the threat detected.

- Information about the operating system: operating system's version, installed service packs, services and drivers being downloaded, versions of browsers and mail clients, browser extensions, version number of the Kaspersky Lab's application installed.

To enable sending statistics in Kaspersky Security Network, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.

2. In the window that will open, select the **Feedback** section and check the **I agree to participate in Kaspersky Security Network** box.

APPLICATION'S APPEARANCE

You can change the appearance of Kaspersky PURE by creating and using various graphics and color schemes. Also, using various active interface elements can be configured (such as the application icon in the Microsoft Windows taskbar notification area, or pop-up messages).

SEE ALSO:

ACTIVE INTERFACE ELEMENTS

To configure the active interface elements (such as the Kaspersky PURE icon in the system tray and pop-up messages), you can use the following features of Kaspersky PURE:

Animate taskbar icon when executing tasks.

Depending on the operation being performed by the application, the application icon in the system tray will change. For example, if an email message is being scanned, a small depiction of the letter appears in the background of the icon. The Kaspersky PURE icon is animated. In this case, it will only reflect your computer's protection status: if the protection is enabled, the icon will be colored, if it is paused or disabled – it will be grey.

Use semi-transparent windows.

All the application's operations which require your immediate attention or your decision are presented as pop-up messages displayed above the application icon in the system tray. The message windows are translucent so as not to interfere with your work. When pointed with the mouse cursor, the message window's loses its translucency.

Enable news notifications.

By default, when some news are received, the system tray will display a special icon which, when clicked, displays a window containing the piece of news.

Show "Protected by Kaspersky Lab" on Microsoft Windows logon screen.

By default, this indicator appears in the top right corner of the screen when Kaspersky PURE starts. It informs you that your computer is protected from any type of threats.

If the application is installed on the computer running under Microsoft Windows Vista, this option will be unavailable.

To configure active interface elements, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that will open, select the **Appearance** section.
3. In the **Icon in the taskbar notification area** block, check or uncheck the required boxes.

KASPERSKY PURE SKIN

All colors, fonts, icons, and texts used in Kaspersky PURE interface can be modified. You can create your own skins for the application, or localize it in another language.

To use another application skin, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that will open, select the **Appearance** section.
3. Check the **Use alternative skin** box in the **Skins** section to activate a skin. Specify the folder with the skin settings in the entry field. To select the folder, click the **Browse** button.

GAMING PROFILE

Using some applications (such as gaming programs) in full-screen mode may lead to the need of disabling certain functions of Kaspersky PURE, such as the notification service. Additionally, those applications often require significant system resources, so that executing certain Kaspersky PURE's tasks may slow down their performance.

To avoid manually disabling notifications and pausing tasks every time you are launching full-screen applications, Kaspersky PURE provides the option of temporarily editing the settings using the gaming profile. The gaming profile allows simultaneously editing the settings of all the components when switching to full-screen mode, and rolling back the changes made when exiting the mode.

When switching to full-screen mode, event notifications will be disabled automatically. Additionally, you can specify the following settings:

- **Select action automatically**. If this setting is selected, the automatic selection of action will be applied to all the components as a reaction even if the **Prompt for action** option is selected in their settings. So, the user will not receive offers to select an action on the detected threats, as the application will select the action automatically.
- **Do not run updates**, **Do not run scheduled scan tasks**, and **Do not run backup tasks**. These settings are recommended to use in order to avoid slowing down the performance of full-screen applications.

To enable the gaming profile, please do the following:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that will open, select the **Gaming profile** section.
3. Check the **Use Gaming profile** box and specify the required settings.

APPLICATION SETTINGS MANAGEMENT

In this window, you can use the following advanced functions of Kaspersky PURE:

- Exporting / importing Kaspersky PURE settings (see page 255).

- Restoring the default settings of Kaspersky PURE (see page 255).

EXPORTING / IMPORTING KASPERSKY PURE SETTINGS

Kaspersky PURE can import and export its settings.

This is a helpful feature when, for example, Kaspersky PURE is installed on your home computer and in your office. You can configure the application the way you want it at home, export those settings as a file on a disk, and using the import feature, load them on your computer at work. The settings are stored in a special configuration file.

To export the current settings of Kaspersky PURE, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Application settings management** section and click the **Save** button.
3. In the window that will open enter the name of the configuration file and the path where it should be saved.

To import the application's settings from a saved configuration file:

1. Open the main application window and click the **Settings** link in the top part.
2. In the window that will open, select the **Application settings management** section and click the **Load** button.
3. In the window that will open, select the file from which you want to import the Kaspersky PURE settings.

RESTORING DEFAULT SETTINGS

You can always return to the default or recommended Kaspersky PURE settings. They are considered optimum, and are recommended by Kaspersky Lab. Application Configuration Wizard restores default settings.

In the window that will open, you will be asked to determine which settings and for which components should or should not be saved when restoring the recommended security level.

The list shows which components of Kaspersky PURE have settings that differ from the default values, either because they have been modified by the user, or through accumulated training by Kaspersky PURE (Firewall or Anti-Spam). If special settings have been created for any of the components, they will also be shown on the list.

Examples of special settings would be: white and black lists of phrases and addresses used by Anti-Spam, lists of trusted addresses and trusted ISP telephone numbers, exclusion rules created for application components, and Firewall's packet and application filtering rules.

These lists are created when working with Kaspersky PURE with regard to individual tasks and security requirements. Creating them may take a long time, so you are advised to save them before restoring the application's default settings.

After you are finished with the Configuration Wizard, the **Recommended** security level will be set for all components, except for the settings that you have decided to keep customized when restoring. In addition, the settings that you have specified when working with the Wizard will also be applied.

To restore protection settings, please do the following:

1. Open the main application window and click the **Settings** link in the top part of the window.
2. In the window that will open, select the **Application settings management** section and click the **Restore** button.
3. In the window that will open, check the boxes for the settings requiring to be saved. Click the **Next** button. This will run the Application Configuration Wizard. Follow its instructions.

NOTIFICATIONS

When runtime events occur, special notification messages are displayed on the screen. Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alarm**. A critical event has occurred, for instance, a malicious object or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. The notification window of this type is of the red color.

- **Warning**. A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide on how dangerous you think this action is. The notification window of this type is of the yellow color.

- **Info**. This notification gives information about non-critical events. The notification window of this type is of the green color.

The notification window consists of four parts:

1. *Window heading*. The notification window heading contains a brief description of the event, for example: request for rights, suspicious activity, new network, alert, virus.

2. *Event description*. The event description section displays detailed information about the reason for the notification to have appeared: name of the application which caused the event, name of the threat detected, settings of the detected network connection, etc.

3. *Action selection area*. In this section you will be offered to select one of the actions available for this event. Suggested options for the action depend on the event type, for example: **Disinfect**, **Delete**, **Skip –** if a virus was detected, **Allow**, **Block –** in case of the application's request to obtain rights for executing potentially harmful actions. The action recommended by Kaspersky Lab's experts will be displayed in bold typeface.

   If you select **Allow** or **Block**, the window will open where you will be able to select the *action application mode*. For the **Allow** action you can select one of the following modes:

   - **Allow always**. Select this option in order to allow activities of the program by entering changes into the rule of the program's access to the system resources.

   - **Allow now**. Select this option to apply the selected action to all similar events detected during the application's session. Application session is the time since the moment it was started until the moment it was closed or restarted.

   - **Make trusted**. Select this option to move the application to the **Trusted** group.

   For the **Block** action you can select one of the following modes:

   - **Block always**. Select this option in order to block activities of the program by entering changes into the rule of the program's access to the system resources.

   - **Block now**. Select this option to apply the selected action to all similar events detected during the application's session. Application session is the time since the moment it was started until the moment it was closed or restarted.

   - **Terminate**. Select this option to interrupt the program's operation.

4. *Additional action selection area*. Using this section you can select an additional action:

   - **Add to exclusions**. If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to avoid the program making repeat false positives when you use the object.

   - **Apply to all objects**. Check this box to force the specified action to be applied to all objects with the same status in similar situations.

IN THIS SECTION:

OBJECT CANNOT BE DISINFECTED

There are some cases when it is impossible to disinfect a malicious object. This could happen if a file is so damaged that it is impossible to delete malicious code from it and restore integrity. The treatment procedure cannot be applied to several types of dangerous objects, such as Trojans.

In such cases, a special notification will pop up containing:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.

- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.

- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

  You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan task until it is complete.

UNAVAILABLE UPDATE SERVER

If one or several networked computers use a currently unavailable computer as an update server, regular update of Kaspersky PURE is impossible. In this case, network security is put in jeopardy, and Kaspersky PURE displays a corresponding message in the network protection state report.

To ensure safe operation, turn on the unavailable computer or assign another update source.

MALICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects malicious code, a special notification will pop up.

It contains:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.

- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Disinfect** – attempt to disinfect the malicious object. Before treatment, a backup copy is made of the object in case the necessity arise to restore it or a portrait of its infection.

- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.

- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

  You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

DANGEROUS OBJECT DETECTED IN TRAFFIC

When Web Anti-Virus detects a malicious object in traffic, a special notification pops up on screen.

The notification contains:

- The threat type (for instance, *virus modification*) and the name of the dangerous object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the object is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.

- Full name of the dangerous object and a path to the webpage.

You are asked to select one of the following responses to the object:

- **Allow** – continue the object downloading.

- **Block** – block the object downloading from the web resource.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

SUSPICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects an object containing code from an unknown virus or modified code of a known virus, a special notification will pop up.

It contains:

- The threat type (for instance, *virus*, *Trojan*) and the name of the object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.

- Full name of the object and a path to it.

You are asked to select one of the following responses to the object:

- **Quarantine** – move the object to the quarantine. When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk or email, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

  When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

- **Delete** – delete the object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.

- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

  You can later come back to skipped objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to avoid the program making repeat false positives when you use the object.

DANGEROUS ACTIVITY DETECTED IN THE SYSTEM

When Proactive Defense detects dangerous application activity on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.

- Full name of the file of the process that initiated the dangerous activity and a path to it.

- Possible responses:

- **Quarantine** – shuts down the process and places the executable file to the quarantine. When you place an object in Quarantine, it is moved, not copied. Files in Quarantine are saved in a special format and are not dangerous.

  When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

- **Terminate** – shuts down the process.

- **Allow** – allows the process to execute.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to prevent Computer Protection from making repeat false positives when detecting it.

HIDDEN PROCESS DETECTED

When Proactive Defense detects a hidden process on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.

- Full name of the hidden process file and a path to it.

- Possible responses:

  - **Quarantine** – move the process' executable file to quarantine. When you place an object in Quarantine, it is moved, not copied. Files in Quarantine are saved in a special format and are not dangerous.

    When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

    If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

  - **Terminate** – shuts down the process.

  - **Allow** – allows the process to execute.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to prevent Computer Protection from making repeat false positives when detecting it.

ATTEMPT TO ACCESS THE SYSTEM REGISTRY DETECTED

When Proactive Defense detects an attempt to access system registry keys, a special notification pops up containing:

- The registry key being accessed.
- Full name of the file of the process that initiated the attempt to access the registry keys and a path to it.
- Possible responses:
  - **Allow** – allows to execute the dangerous action once;
  - **Block** – blocks the dangerous action once.

To perform the action you have selected automatically every time this activity is initiated on your computer, check the **Create a rule** box.

If you are sure that any activity by the application that attempted to access system registry keys is not dangerous, add the application to the trusted application list.

NETWORK ACTIVITY OF AN APPLICATION HAS BEEN DETECTED

If any network activity of an application is detected (default option for the applications included in the **Low Restricted** or **High Restricted** groups) (see section "Application groups" on page 88), a notification will be displayed on the screen.

A notification will be displayed if My Computer Protection is running in interactive mode (see section "Using interactive protection mode" on page 156), and if no packet rule has been created for the application whose network activity had been detected (see page 103).

The notification contains:

- *Activity description* – name of the application and general features of the connection it initiates. Generally, the connection type, local port from which it is being initiated, remote port, and address being connected to are given.
- *Application run sequence*.
- *Action* – series of operations that Computer Protection should perform regarding the network activity detected.

You are asked to select one of the following actions:

- **Allow**.
- **Deny**.
- **Create a rule**. When this option is selected, *Rule Creation Wizard* (see page 104) is started, which will help you to create a rule, controlling network activity of the application.

You can:

- Perform an action only once. To do so, select **Allow** or **Deny**.
- Apply an action to the session of the application whose network activity has been detected. To do so, select **Allow** or **Deny**, and check the **Apply to current application session** box.

- Apply the action selected for the application to all sessions. To do so, select **Allow** or **Deny**, and check the **Apply always**.

- Create a rule to regulate the application's network activity. To do so, select **Create a rule**.

NEW NETWORK DETECTED

Every time your computer connects to a new zone (i.e. network), a special notification will pop up.

The upper portion of the notification contains a brief description of the network, specifying the IP address and subnet mask.

The lower part of the window requests you to assign a status to the zone, and network activity will be allowed based on that status:

- **Public network (block external access to computer)**. A high-risk network in which your computer is in danger of any possible type of threat. It is recommended to select this status for networks not protected by any anti-virus applications, firewalls, filters etc. When you select this status, the program ensures maximum security for this zone.

- **Local network (allow access to files and printers)**. This status is recommended for zones with an average risk factor (for example, corporate LANs).

- **Trusted network (allow any network activity)**. It is only recommended to apply this status to zones that in your opinion are absolutely safe where your computer is not subject to attacks and attempts to gain access to your data.

PHISHING ATTACK DETECTED

Every time Computer Protection detects a phishing attack, a special notification will pop up.

The notification will contain:

- The name of the threat (*phishing attack*) as a link to the Kaspersky Lab's Virus Encyclopedia with a detailed overview of the threat.

- The web address for the phishing attack.

- Possible responses:

  - **Allow** – continues phishing site downloading.

  - **Block** – blocks phishing site downloading.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

SUSPICIOUS LINK DETECTED

Every time Computer Protection detects an attempt to open the website, the address of which is contained in the list of suspicious web addresses, a special notification will pop up.

The notification will contain:

- The website address.

- Possible responses:
  - **Allow** – continues the website download.
  - **Block** – blocks the website download.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan until it is complete.

INVALID CERTIFICATE DETECTED

Security check for the connection via SSL protocol is performed using the installed certificate. If an invalid certificate is detected when the connection to the server is attempted (for example, if the certificate is replaced by an intruder), a notification will be displayed on screen.

The notification will contain the information about possible cause of error, and will identify remote port and address. You will be prompted to decide if the connection with an invalid certificate should be continued:

- **Accept certificate** – continue connection with the website;
- **Reject certificate** – interrupt connection with the website;
- **View certificate** – view information about certificate.

LIMITING USING THE APPLICATION

If a time restriction on the use of application was specified in the Parental Control, a special notification will be displayed on the screen when the specified time elapses.

The following information will be displayed in the notification:

- application name;
- time before the application ends, or the reason for the application to end.

SPECIAL TREATMENT REQUIRED

When you detect a threat that is currently active in the system (for example, a malicious process in RAM or in startup objects), a message will pop up prompting you to carry out a special advanced disinfection procedure.

The Kaspersky Lab specialists strongly recommend that you agree with to carry out the advanced disinfection procedure. To do so, click the **OK** button. However, note that your computer will restart once the procedure is complete, so we recommend saving your current work and closing all applications before running the procedure.

While the disinfection procedure is running, email client or operating system registry editing sessions cannot be started. After restarting your computer, you are advised to run the full virus scan.

FILE ALREADY EXISTS

If, during restoration of a file from its backup copy, a file with such name already exists in the chosen folder, a special notification will be displayed on the screen.

In the top part of the notification window, the file name and location will be specified.

In the bottom part of the window, you will be offered to specify the method of file restoration:

- **Replace**. The file you are restoring will replace the existing file.
- **Skip**. The current file version will be saved.
- **Save both files**. The file you are restoring will be assigned another name.

ELIMINATING PROBLEMS

If problems occur in Kaspersky PURE operation, first of all check if the method for solving them is described in the application Help system or in the Kaspersky Lab Knowledge Basehttp://support.kaspersky.ru). The *Knowledge Base* is a separate section of the Technical Support web site, and comprises recommendations for Kaspersky Lab products as well as answers to frequently asked questions. Try to find an answer to your question or a solution to your problem with this resource.

To use The Knowledge Base:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that opens, click the **Knowledge Base** link.

Another resource you can use to obtain information about working with the application is Kaspersky Lab users forum. It is another separate section of the Technical Support web site and it contains user questions, feedback and requests. You can view the main topics of the forum, leave feedback or find an answer to a question.

To open the users' forum:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that opens, click the **User Forum** link.

If you cannot find a solution to your problem in the application Help system, in the Knowledge Base, or at the User Forum, we recommend that you contact Kaspersky Lab Technical Support.

IN THIS SECTION:

CREATING A SYSTEM STATE REPORT

When solving your problems Kaspersky Lab's specialists may require a report about the system state. This report contains detailed information about running processes, loaded modules and drivers, Microsoft Internet Explorer and Microsoft Windows Explorer plug-ins, open ports, detected suspicious objects, etc.

When a system state report is created no user personal information is collected.

To create a system state report:

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that opens, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that opens, click the **Create system state report** button.

The system state report is created in *HTML* and *XML* formats and is saved in *sysinfo.zip* archive. Once the information gathering process is complete, you can view the report.

To view the report:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that opens, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that opens, click the **View** button.

5. Open the *sysinfo.zip* archive, which contains report files.

SENDING DATA FILES

After you have created the tracing files and the system state report you will have to send them to Kaspersky Lab's support experts.

You will need a request number to upload data files to the Technical Support server. This number is available in your Personal Cabinet on the Technical Support website if your request is active.

In order to upload the data files to the Support service server:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that opens, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that opens, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

5. In the window that will open check boxes next to the tracing files you wish to send to the Support service and click the **Send** button.

6. In the **Enter request number** window that opens, specify the number assigned to your request when filling in the electronic form on the Support Service website.

The selected tracing files will be packed and sent to the Support Service server.

If for some reason you cannot contact Technical Support Service you can save the data files on your computer.

To save data files to the disk:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that opens, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that opens, in the **Actions** section, click the **Upload information for Technical Support Service to the server** button.

5. In the window that will open check boxes next to the tracing files you wish to send to the Support service and click the **Send** button.

6. In the **Enter request number** window that opens, click the **Cancel** button and confirm saving files to the disk.

7. Specify the archive name in the window that will open.

Later on you will be able to send the saved files to Technical Support with the help of My Kaspersky Account (https://support.kaspersky.com/ru/personalcabinet?LANG=en).

EXECUTING AVZ SCRIPT

Kaspersky Lab experts will analyze your problem using the tracing files and the system state report. The outcome of the analysis is a sequence of actions aimed at eliminating the problems detected. The list of such actions can be rather long.

To simplify the procedure, AVZ scripts are used. An AVZ script is a set of instructions allowing to edit registry keys, quarantine files, search for classes of files and potentially quarantine files related to them, block UserMode and KernelMode interceptors, and etc.

To run the scripts the application includes an *AVZ script execution wizard*. This wizard consists of a series of screens (steps) navigated using the **Back** and the **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any stage, use the **Cancel** button.

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, please contact Technical Support service.

To start the wizard:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that opens, click the **Support tools** link in the bottom part of the window.

4. In the **Information for Technical Support Service** window that opens, click the **Execute AVZ script** button.

If the script successfully executes, the wizard will close. If an error occurs during script execution, the wizard displays a corresponding error message.

CREATING A TRACE FILE

After installing Kaspersky PURE, some failures in the operating system or in the operation of individual applications may occur. The most likely cause is a conflict of Kaspersky PURE with the software installed on your computer, or with the drivers of your computer components. You may be asked to create a tracing file for Kaspersky Lab's specialists to successfully resolve your problem.

To create the trace file:

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.

3. In the **Support** window that opens, click the **Support tools** link.

4. In the **Information for Technical Support Service** window that opens, use the dropdown list in the **Traces**, section to select the tracing level. The tracing level should be set on the advice of the Technical Support specialist. If no indications from Technical Support are available, you are advised to set tracing level to **500**.

5. To start the tracing process, click the **Enable** button.
6. Reproduce the situation which caused the problem to occur.
7. To stop the tracing process, click the **Disable** button.

You can switch to uploading tracing results to Kaspersky Lab's server.

CONTACTING THE TECHNICAL SUPPORT SERVICE

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

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

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

An email request to the Technical Support Service

You can ask your question in Russian, English, German, French or Spanish.

The Technical Support Service will reply to your request in your Kaspersky Account (https://my.kaspersky.com/ru/index.html?LANG=en) and to the email address you have specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. Specify the following in the mandatory fields:

- **Request type**. Select the subject that corresponds to the problem the most strictly, for example: Problem with product installation/uninstallation, or Problem with searching/eliminating viruses. If you have not found an appropriate topic, select "General Question".
- **Application name and version number**.
- **Request text**. Describe the problem you have encountered providing as much details as possible.
- **Customer ID and password**. Enter the client number and the password you have received during the registration at the Technical Support service website.
- **Email address**. The Technical Support service will send an answer to your question to this email address.

Technical support by phone

If you have an urgent problem you can call your local Technical Support service at +7 (495) 663-81-47. Before contacting technical support specialists, please collect the information (http://support.kaspersky.com/support/details) about your computer and the anti-virus software on it. This will let our specialists help you more quickly.

KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

This Statement describes the terms of collection and use of the information, specified bellow.

This Statement applies to Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky PURE products belonging to Kaspersky Lab.

In order to detect new data security threats and their sources, to improve user data protection and the functionality of the products developed by Kaspersky Lab, the user can collect information in accordance with the list below after the feature is enabled by the user in the Feedback section of the settings window of each respective product.

List of basic information items:

- Information about computer hardware and software, including operating system version and installed service packs, kernel objects, drivers, services, Microsoft Internet Explorer add-ons, printing system extensions, Windows Explorer plug-ins, loaded objects, Active Setup items, control panel applets, records from the hosts file and system registry, IP addresses, versions of browsers and email clients and the version of Kaspersky Lab product.

- Unique identifier assigned by the product of Kaspersky Lab to the user's computer.

- Information about the status of anti-virus protection on the computer and about all potentially harmful files and operations (including virus name, date and time of its detection, names and sizes of infected files and their paths, IP address of an attacking computer and the number of the port attacked via network, name of a potentially malicious application).

- Information about signed applications downloaded by the user (URL, file size, signature).

- Information about launched applications (size, attributes, creation date, PE header information, region, name, location, packer).

Additionally, the user can provide information in accordance with the list below:

- Files and / or file fragments for additional scan at Kaspersky Lab. Transmission of those files and / or file fragments will be done only if you accept the terms of this agreement.

No personal user data are collected, processed or stored.

Submission of the data mentioned above is voluntary. You can enable or disable the data collection option at any moment in the Feedback section of the settings window of the respective Kaspersky Lab product.

USING THIRD-PARTY CODE

Third-party code was used to develop Kaspersky PURE.

IN THIS SECTION:

AGAVA-CLIBRARY

Agava-C program library, developed by OOO "R-Alpha", is used to check digital signature.

CRYPTO C LIBRARY (DATA SECURITY SOFTWARE LIBRARY)

To create and check the digital signatures, the Crypto C data security software library is used, developed by "CryptoEX", http://www.cryptoex.ru.

FASTSCRIPT 1.9 LIBRARY

When creating the application, the FastScript library copyright © Fast Reports Inc. has been used. All rights reserved.

PCRE 7.4, 7.7 LIBRARY

Library pcre 7.4 copyright © 1997-2008 University of Cambridge under BSD license was used during application development.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR

TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU BISON PARSER LIBRARY

The bison parser skeleton 2.3 copyright © GNU Project http://ftp.gnu.org/gnu/bison/ library under the framework of a special exception was used during application development.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

AGG 2.4 LIBRARY

The AGG (Anti-Grain Geometry) 2.4 copyright © 2002-2005 Maxim Shemanarev library was used during application development. All rights reserved, under modified BSD license.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

OPENSSL 0.9.8D LIBRARY

The OpenSSL 0.9.8d copyright © 1998-2007 The OpenSSL Project library was used during application development. All rights reserved, under OpenSSL License and Original SSLeay License (http://www.openssl.org/).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

GECKO SDK 1.8 LIBRARY

The Gecko SDK 1.8 Copyright © Mozilla Foundation library was used during application development. All rights reserved, under MPL 1.1 license (http://www.mozilla.org/MPL/MPL-1.1.html). Website and link to the distribution package: http://developer.mozilla.org/en/docs/Gecko_SDK.

ZLIB 1.2 LIBRARY

The zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler library was used during application development. All rights reserved, under zlib/libpng license.

LIBPNG 1.2.8, 1.2.29 LIBRARY

The libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson library was used during application development. All rights reserved, under zlib/libpng license.

LIBNKFM 2.0.5 LIBRARY

The libnkfm 2.0.5 Copyright (c) KUBO Takehiro library was used during application development. All rights reserved.

EXPAT 1.2, 2.0.1 LIBRARY

The Expat 1.2, 2.0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. library was used during application development. All rights reserved, used under the following conditions:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

INFO-ZIP 5.51 LIBRARY

The Info-ZIP 5.51 Copyright (c) 1990-2007 library was used during application development. All rights reserved, under Info-ZIP license.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

WINDOWS INSTALLER XML (WIX) 2.0 LIBRARY

The Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation library was used during application development. All rights reserved, under CPL 1.0 license (http://sourceforge.net/projects/wix/).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

PASSTHRU LIBRARY

The Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation library was used during application development. All rights reserved.

FILTER LIBRARY

The Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation library was used during application development. All rights reserved.

NETCFG LIBRARY

The Network Configuration Sample Copyright (c) 1997 Microsoft Corporation library was used during application development. All rights reserved.

PCRE 3.0 LIBRARY

The pcre 3.0 copyright © 1997-1999 University of Cambridge under PCRE LICENSE library was used during application development. All rights reserved.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

The RFC1321-based (RSA-free) MD5 library was used during application development. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. Distributed under zlib/libpng license.

WINDOWS TEMPLATE LIBRARY (WTL 7.5)

The Windows Template Library 7.5 Copyright (c) 2005 Microsoft Corporation was used during application development. All rights reserved, under Common Public license 1.0, http://sourceforge.net/projects/wtl/.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial

Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBJPEG 6B LIBRARY

The libjpeg 6b library was used during application development. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. Is used under the following conditions:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining

code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBUNGIF 3.0 LIBRARY

The libungif 3.0 library was used during application development. Copyright (c) 1997 Eric S. Raymond. Is used under the following conditions:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR LIBRARY

The libxdr copyright © Sun Microsystems, Inc.library was used during application development. Is used under the following conditions:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

TINICONV - 1.0.0 LIBRARY

The tiniconv – 1.0.0 library was used during application development. Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (http://sourceforge.net/projects/tiniconv/) under GNU LGPL 2.1 license (http://www.gnu.org/).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its

terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code

and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BZIP2/LIBBZIP2 1.0.5 LIBRARY

The bzip2/libbzip2 1.0.5 library was used during application development. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. Is used under the following conditions:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

LIBSPF2-1.2.9 LIBRARY

The libspf2-2/1/09 library was used during application development. Copyright 2005 by Shevek and Wayne Schlitt. All rights reserved, used under the conditions of The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PROTOCOL BUFFER LIBRARY

The Protocol Buffer library was used during application development. Copyright 2008, Google Inc. All rights reserved, is distributed under conditions of New BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

SQLITE 3.5.9 LIBRARY

The sqlite 3.5.9 library has been used when creating the application. Copyright (C) Dan Kennedy, D. Richard Hipp, http://www.sqlite.org/copyright.html.

ICU 4.0 LIBRARY

The icu 4.0 library has been used when creating the application. Copyright (c) 1995-2009 International Business Machines Corporation and others. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

OTHER INFORMATION

This product contains or may contain programs that are licensed (or sublicensed) to the user in accordance with the public GNU license or other similar Open Source licenses, which, in addition to other rights, allow the user to copy, modify, or redistribute certain programs or parts thereof, and gain access to the source code (open source software). If such license provides the source code to the users, who receive the software in the form of executable binary code, the source code becomes available when requested by email at source@kaspersky.com, or is supplied with the product.

GLOSSARY

List of masks and addresses of web resources, to which content the user trusts. Kaspersky Lab application does not scan web pages, corresponding to some list item, for the presence of malicious objects.

WHITE LIST

Records in this list contain

- *phone numbers*, whose incoming calls and SMS messages are skipped by Anti-Spam, as well as outgoing calls and SMS messages are skipped by Parental Control.
- *text*, which makes the application skip an incoming SMS message, when detected.

BLACK LIST OF KEY FILES

A database containing information on blacklisted Kaspersky Lab key files whose owners violated the terms of the license agreement and information on key files that were issued but for some reason were not sold or were replaced. A blacklist file is necessary for the operation of Kaspersky Lab applications. File contents is updated together with the databases.

BOOT-VIRUS

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

OLE OBJECT

An attached object or an object embedded into another file. Kaspersky Lab application allows to scan OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table will be scanned as an OLE object.

SOCKS

Proxy server protocol that allows to establish a point-to-point connection between computers in the internal and external networks.

ACTIVATING THE APPLICATION

The application activation procedure consists in entering an activation code and obtaining a key which will allow the application to determine if the user has sufficient rights to use it, and to find out the license expiration date.

ACTIVE LICENSE

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with the active status.

ALTERNATE NTFS STREAMS

NTFS data streams (alternate data streams) designed to contain additional attributes or file information.

Each file in NTFS file system is a set of streams. One of them contain the file content that one will be able to view after opening the file, other streams (called alternate) are designed to contain meta information and ensure, for example, NTFS compatibility with other systems, such as an older file system by Macintosh called Hierarchical File System (HFS). Streams can be created, deleted, stored apart, renamed, and even run as a process.

Alternate streams can be used by intruders to transfer data secretly, or to steal them from a computer.

HARDWARE PORT

Socket on a hardware component of a computer in which a cable or a plug can be connected (LPT port, serial port, USB port).

ARCHIVE

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

BASE OF SUSPICIOUS WEB ADDRESSES

List of web addresses, which content can be considered as potentially dangerous. The list is created by Kaspersky Lab specialists. It is regularly updated and is included into the Kaspersky Lab application package.

BASE OF PHISHING WEB ADDRESSES

List of web addresses, which are defined as phishing by Kaspersky Lab specialists. The base is regularly updated and it is a part of Kaspersky Lab application.

DATABASES

Databases created by Kaspersky Lab's experts and containing detailed description of all currently existing threats to computer security as well as methods used for their detection and disinfection. These databases are constantly updated by Kaspersky Lab as new threats appear. In order to achieve higher quality of threat detection we recommend that you copy databases from Kaspersky Lab's update servers on a regular basis.

BLOCKING THE OBJECT

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

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

POTENTIALLY INFECTED OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected using heuristic analyzer.

RESTORATION

Moving an original object from Quarantine or Backup to the folder where it was originally found before being moved to Quarantine, disinfected, or deleted, or to a different folder specified by the user.

DUAL-HOMED GATEWAY

Computer equipped with two network adapters (each of which is connected to different networks) transferring data from one network to the other.

TRUSTED PROCESS

Application process whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects run, open, or saved by the trusted process will be scanned.

ADDITIONAL LICENSE

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

AVAILABLE UPDATES

A set of updates for Kaspersky Lab application modules including critical updates accumulated over a period of time and changes to the application's architecture.

HEADER

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and the recipient, and the date.

DISK BOOT SECTOR

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disc's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows to scan boot sectors for viruses and disinfect them if an infection is found.

TASK

Functions performed by Kaspersky Lab's application are implemented as tasks, such as: **Real-time file protection**, **Full computer scan**, **Database update**.

INFECTED OBJECT

Object containing a malicious code. It is detected when a section of the object's code completely matches a section of the code of a known threat. Kaspersky Lab does not recommend using such objects since they may cause your computer to be infected.

EXCLUSION

Exclusion is an object excluded from the scan by Kaspersky Lab application. You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects by threat type according the Virus Encyclopedia classification. Each task can be assigned a set of exclusions.

QUARANTINE

A certain folder into which all possibly infected objects are placed, which were detected during scans or by real-time protection.

MONITORED OBJECT

A file transferred via HTTP, FTP, or SMTP protocols across the firewall and sent to a Kaspersky Lab application to be scanned.

OBJECT DISINFECTION

The method used for processing infected objects that results in complete or partial recovery of data, or the decision that the objects cannot be disinfected. Disinfection of objects is performed using the database records. Part of the data may be lost during disinfection.

DISINFECTING OBJECTS ON RESTART

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original infected object with the disinfected copy after the next system restart.

FALSE ALARM

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

SUBNET MASK

Subnet mask (also known as netmask) and network address determine the addresses of computers on a network.

FILE MASK

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

UNKNOWN VIRUS

A new virus about which there is no information in the databases. Generally unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

INCOMPATIBLE APPLICATION

An anti-virus application from a third-party vendor or a Kaspersky Lab application that does not support management via Computer Protection.

OBSCENE MESSAGE

Email message containing offensive language.

UPDATE

The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

DATABASE UPDATES

One of the functions performed by a Kaspersky Lab application that enables it to keep protection current. In doing so, the databases are downloaded from the Kaspersky Lab update servers onto the computer and are automatically connected to the application.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which could lead to, for example, blocking your access to the operating system.

DANGEROUS OBJECT

Object containing a virus. You are advised not to access these objects, because it may result in an infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

TASK SETTINGS

Application settings which are specific for each task type.

APPLICATION SETTINGS

Application settings which are common for all task types, regulating the application's operation as a whole, such as application performance settings, report maintenance settings, backup storage settings.

INTERCEPTOR

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

SUSPICIOUS MESSAGE

Message that cannot be unambiguously considered spam, but it seems suspicious when scanned (e.g., certain types of mailings and advertising messages).

SUSPICIOUS OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Suspicious objects are detected using the heuristic analyzer.

MOVING OBJECTS TO QUARANTINE

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection.

VIRUS ACTIVITY THRESHOLD

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, will be considered excessive virus activity and a threat of a virus outbreak. This feature is significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

INPUT/OUTPUT PORT

Serves in processors (such as Intel) for exchanging data with hardware components. Input/output port is associated with a certain hardware component, and allows applications to address it for data exchange.

REAL-TIME PROTECTION

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

POTENTIALLY INFECTIBLE OBJECT

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the **.com**, **.exe**, **.dll** extensions, etc. The risk of activating any malicious code in such files is fairly high.

MAIL DATABASES

Databases containing emails in a special format and saved on your computer. Each incoming/outgoing email is placed in the mail database after it is received/sent. These databases are scanned during a full computer scan.

Incoming and outgoing emails at the time that they are sent and received are analyzed for viruses in real time if real-time protection is enabled.

TRAFFIC SCAN

A real-time scan using information from the latest version of the databases for objects transmitted over all protocols (for example, HTTP, FTP, etc.).

APPLICATION MODULES

Files included in the Kaspersky Lab installation package responsible for performing its main tasks. A particular executable module corresponds to each type of the task performed by the application (real-time protection, on-demand scan, updates). By running a full scan of your computer from the main window, you initiate the execution of this task's module.

PROXY SERVER

Computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then, the proxy server either connects to the specified server and obtains the resource from it, or returns the resource from its own cache (in case if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server in certain reasons.

PROTOCOL

Clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP (WWW), FTP, and NNTP (news).

INTERNET PROTOCOL (IP)

The base protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations in transmitting data from one computer to another and serves as a foundation for higher-level protocols like TCP and UDP. It manages the connection and error processing. Technologies such as NAT and masking make it possible to hide a large number of private networks using a small number of IP addresses (or even one address), which make it possible to respond to the demands of the constantly growing Internet using the relatively restricted IPv4 address space.

BACKUP COPY

Creating a backup copy of a file before any processing and putting the copy into the backup storage area with the possibility of restoring the file later, for example, to scan it with updated databases.

BACKUP STORAGE

Special storage designed to save backup copies of objects created before their first disinfection or deletion.

RECOMMENDED LEVEL

Level of security based on application settings recommended by Kaspersky Lab experts to provide the optimal level of protection for your computer. This level is set to be used by default.

KASPERSKY LAB'S UPDATE SERVERS

A list of Kaspersky Lab's HTTP and FTP servers from which the application downloads databases and module updates to your computer.

ADMINISTRATION SERVER CERTIFICATE

Certificate which allows Administration server authentication when connecting Administration console to it and when exchanging data with users' computers. Administration server certificate is created at the installation of Administration server, and is stored in the **Cert** subfolder of the application installation folder.

NETWORK PORT

TCP and UDP parameter that determines the destination of data packets in IP format that are transmitted to a host over a network and makes it possible for various programs running on a single host to receive data independently of each other. Each program processes data received via certain port (this is sometimes referred to as the program "listening" to that port).

For some common network protocols there are usually standard port numbers (for example, web servers usually receive HTTP requests on TCP port 80); however, generally, a program can use any protocol on any port. Possible values: 1 to 65535.

SCRIPT

A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a small specific task. It is most often used with programs embedded into hypertext. Scripts are run, for example, when you open a certain website.

If real-time protection is enabled, the application will track the scripts launching, intercept them, and scan for viruses. Depending on the results of the scan you can block or allow the execution of a script.

DOMAIN NAME SERVICE (DNS)

Distributed system for converting the name of a host (a computer or other network device) into IP address. DNS functions in TCP/IP networks. Particularly, DNS can also store and process reverse requests, by determining the name of a host by its IP address (PTR record). Resolution of DNS names is usually carried out by network applications, not by users.

SPAM

Unsolicited mass email mailings, most often including advertising messages.

LIST OF BLOCKED WEB ADDRESSES

List of masks and addresses of web resources, access to which is blocked by Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

LIST OF BLOCKED SENDERS

(also "Black" list of addresses)

The list of email addresses which send the messages that should be blocked by Kaspersky Internet Security, regardless of their content.

LIST OF CHECKED WEB ADDRESSES

List of masks and addresses of web resources, which are mandatory scanned for malicious objects by Kaspersky Lab application.

LIST OF ALLOWED WEB ADDRESSES

List of masks and addresses of web resources, access to which is not blocked by Kaspersky Lab application. The list of addresses is created by the user during application settings configuration.

LIST OF ALLOWED SENDERS

(as well as "White" list of addresses)

The list of email addresses which send the messages that should not be scanned by Kaspersky Lab application.

LICENSE VALIDITY PERIOD

Period of time during which you are able to use all of the features of your Kaspersky Lab's application. License validity period generally accounts for one calendar year from the date of its installation. After the license expires, the application will have reduced functionality. You will not be able to update the application databases.

URGENT UPDATES

Critical updates to Kaspersky Lab application modules.

PROTECTION STATUS

The current status of protection, summarizing the degree of security of the computer.

VIRUS OUTBREAK COUNTER

Template based on which a notification of virus outbreak threat is generated. Virus outbreak counter includes a combination of settings which determine the virus activity threshold, the way of spreading, and the text in messages to send.

ICHECKER TECHNOLOGY

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remain unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive scanned by Kaspersky Lab application and assigned the *not infected* status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive will be re-scanned.

Limitations of **iChecker** technology:

- this technology does not work with large-size files since it is faster to scan a file than check whether it was modified since it was last scanned;
- the technology supports a limited number of formats (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

DELETING AN OBJECT

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for any reason, cannot be disinfected.

MESSAGE DELETION

Method of processing an email message that contains spam signs, at which the message is physically removed. This method is advised to apply to messages unambiguously containing spam. Before deleting a message, a copy of it is saved in the backup (unless this option is disabled).

COMPRESSED FILE

An archive file that contains a decompression program and instructions for the operating system for executing.

SECURITY LEVEL

The security level is defined as a pre-set component configuration.

EVENT SEVERITY LEVEL

Description of the event, logged during the operation of Kaspersky Lab application. There exist four severity levels:

- **Critical event**.
- **Functional failure**.
- **Warning**.
- **Informational message**.

Events of the same type may have different severity levels, depending on the situation when the event occurred.

INSTALLATION WITH A STARTUP SCENARIO

Method of remote installation of Kaspersky Lab's applications which allows assigning the startup of remote installation task to an individual user account (or to several user accounts). Registering a user in a domain leads to an attempt to install the application on the client computer on which the user has been registered. This method is recommended for installing the applications on computers running under the Microsoft Windows 98 / Me operating systems.

KEY FILE

File with the .key extension, which is your personal "key", necessary for working with Kaspersky Lab application. A key file is included with the product package if you purchase it from Kaspersky Lab distributors; otherwise, it is emailed to you if you purchase the product online.

NOTIFICATION TEMPLATE

Template based on which a notification of infected objects detected by the scan, is generated. Notification template includes a combination of settings regulating the mode of notification, the way of spreading, and the text of messages to send.

HEURISTIC ANALYZER

Threat detection technology for threats that cannot be detected using Anti-Virus databases. It allows detecting objects suspected of being infected with an unknown virus or a new modification of the known viruses.

The use of heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian 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 office, 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).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate 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. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

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. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide 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 design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. 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. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.viruslist.com
Anti-Virus Lab:	newvirus@kaspersky.com (only for sending archives of suspicious objects) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (for queries to virus analysts)
Kaspersky Lab web forum:	http://forum.kaspersky.com

INDEX

A

B

C

D

E

F

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W