Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

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

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial, or personal use.

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

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used herein the rights to which are owned by third parties, or for any potential damages associated with the use of such documents.

Document revision date: 12/4/2012

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

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

**ABOUT THIS GUIDE** ........................................................................................................... 6  
In this guide .......................................................................................................................... 6  
Document conventions ........................................................................................................ 7  

**SOURCES OF INFORMATION ABOUT THE APPLICATION** .............................................. 9  
Sources of information to research on your own ................................................................. 9  
Discussing Kaspersky Lab applications on the Forum .......................................................... 10  
Contacting the Sales Department ....................................................................................... 10  
Contacting Technical Writing and Localization Unit by email ......................................... 10  

**KASPERSKY PURE** .......................................................................................................... 11  
What's new ............................................................................................................................ 11  
Main functions and applications ....................................................................................... 12  
Distribution kit .................................................................................................................. 14  
Service for users ................................................................................................................ 14  
Hardware and software requirements ............................................................................... 15  

**INSTALLING AND REMOVING THE APPLICATION** ....................................................... 16  
Installing the application ..................................................................................................... 16  

**INS**  
Step 1. Finding a newer version of the application ............................................................... 17  
Step 2. Starting the application installation ......................................................................... 17  
Step 3. Reviewing the End User License Agreement ............................................................ 17  
Step 4. Kaspersky Security Network Data Collection Statement .......................................... 17  
Step 5. Installation ............................................................................................................... 17  
Step 6. Completing installation ............................................................................................ 18  
Step 7. Activating the application ....................................................................................... 18  
Step 8. User registration ..................................................................................................... 19  
Step 9. Completing activation ............................................................................................... 19  

**Upgrading previous version of Kaspersky PURE** ............................................................ 19  
Step 1. Finding a newer version of the application ............................................................... 20  
Step 2. Starting the application installation ......................................................................... 20  
Step 3. Reviewing the End User License Agreement ............................................................ 20  
Step 5. Installation ............................................................................................................... 20  
Step 6. Completing installation ............................................................................................ 21  

**Removing the application** ............................................................................................... 22  
Step 1. Saving data for future use ....................................................................................... 22  
Step 2. Confirm removal ..................................................................................................... 23  
Step 3. Removing the application. Completing removal ...................................................... 23  

**APPLICATION LICENSING** ............................................................................................. 24  
About the End User License Agreement ........................................................................... 24  
About the license ................................................................................................................. 24  
About data provision ........................................................................................................... 25  
About the activation code .................................................................................................... 26  

**PERFORMING COMMON TASKS** .................................................................................... 27  
Activating the application ................................................................................................... 28  
Purchasing and renewing a license ..................................................................................... 28
Managing application notifications................................................................. 29
Assessing the computer protection status and resolving security issues.......................... 30
Updating databases and application modules.................................................... 31
Scanning critical areas of your computer for viruses........................................... 32
Full scan of the computer for viruses.............................................................. 32
Scanning a file, folder, disk, or another object for viruses...................................... 33
Scanning the computer for vulnerabilities....................................................... 34
Restoring a file deleted or disinfected by the application....................................... 34
Recovering the operating system after infection................................................ 36
Blocking unwanted email (spam) ..................................................................... 38
Scanning email and filtering attachments in email messages................................. 38
Assessing the safety status of a website............................................................. 39
Blocking access to websites of various regions.................................................... 40
Remote management of home network protection.............................................. 40
Handling unknown applications........................................................................ 41
  Controlling application activities on the computer and on the network................ 41
  Checking application reputation...................................................................... 42
Protecting privacy data against theft................................................................... 43
  Safe Money ..................................................................................................... 44
  Protection against phishing............................................................................ 45
Using Virtual Keyboard...................................................................................... 46
Secure keyboard input ...................................................................................... 48
Password protection .......................................................................................... 49
  Adding account data for automatic login ....................................................... 49
  Using Password Generator ........................................................................... 50
  Adding a new login and password pair ........................................................ 51
Data encryption ................................................................................................. 52
Unused Data Cleaner ....................................................................................... 53
File Shredder .................................................................................................... 55
Privacy Cleaner .................................................................................................. 57
Backup copying.................................................................................................. 59
Data Backup....................................................................................................... 59
Restoring data from a backup copy..................................................................... 60
Using Online storage.......................................................................................... 61
Password-protecting access to Kaspersky PURE settings......................................... 62
Using Parental Control....................................................................................... 63
  Configuring Parental Control ....................................................................... 64
  Viewing the report on a user's activity .......................................................... 64
Pausing and resuming computer protection....................................................... 65
Viewing computer protection report................................................................... 66
Restoring the default application settings.......................................................... 66
Importing the application settings to Kaspersky PURE installed on another computer .............................................................................. 69
Creating and using a Rescue Disk...................................................................... 69
  Creating a Rescue Disk .................................................................................. 70
  Booting the computer using the Rescue Disk ............................................... 72
CONTACTING THE TECHNICAL SUPPORT SERVICE......................................... 73
How to obtain technical support......................................................................... 73
Technical support by phone................................................................................ 73
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining technical support via My Kaspersky Account</td>
<td>74</td>
</tr>
<tr>
<td>Creating a system state and AVZ script usage report</td>
<td>75</td>
</tr>
<tr>
<td>Creating a system state report</td>
<td>75</td>
</tr>
<tr>
<td>Collecting technical data on application performance</td>
<td>76</td>
</tr>
<tr>
<td>Sending data files</td>
<td>76</td>
</tr>
<tr>
<td>AVZ script execution</td>
<td>77</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>78</td>
</tr>
<tr>
<td>KASPERSKY LAB ZAO</td>
<td>85</td>
</tr>
<tr>
<td>INFORMATION ABOUT THIRD-PARTY CODE</td>
<td>86</td>
</tr>
<tr>
<td>TRADEMARK NOTICES</td>
<td>86</td>
</tr>
<tr>
<td>INDEX</td>
<td>87</td>
</tr>
</tbody>
</table>
ABOUT THIS GUIDE

This document is the User Guide to Kaspersky PURE.

For proper use of Kaspersky PURE, you should be acquainted with the interface of the operating system that you use, handle the main techniques specific for that system, know how to work with email and the Internet.

This Guide is intended to do the following:

- Help you install, activate, and use PURE.
- Ensure a quick search of information on application-related issues.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION

In this guide......................................................................................................................................................6
Document conventions ..............................................................................................................................................7

IN THIS GUIDE

This document contains the following sections.

Sources of information about the application

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

Kaspersky PURE

This section contains a description of the application's features and brief information on the application's functions and components. You will learn what items are included in the distribution kit and what services are available for registered users of the application. This section provides information about software and hardware requirements that a computer should meet to allow a user to install the application on it.

Installing and removing the application

This section contains step-by-step instructions for application installation and removal.

Application licensing

This section contains information about the basic concepts of application activation. Read this section to learn more about the purpose of the End User License Agreement, license types, ways of activating the application, and the license renewal.

Performing common tasks

This section contains step-by-step instructions for performing typical user tasks that the application provides.
Contacting the Technical Support Service

This section provides information about how to contact the Technical Support Service at Kaspersky Lab.

Applications

This section provides information that complements the document text.

Glossary

This section contains a list of terms that are mentioned in the document and their definitions.

Kaspersky Lab ZAO

The section provides information on Kaspersky Lab ZAO.

Information about third-party code

This section provides information about the third-party code used in the application.

Trademark notices

This section lists trademarks of third-party manufacturers that were used in the document.

Index

This section allows you to quickly find required information within the document.

**DOCUMENT CONVENTIONS**

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. The following table shows document conventions and examples of their use.

<table>
<thead>
<tr>
<th>SAMPLE TEXT</th>
<th>DESCRIPTION OF DOCUMENT CONVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that...</td>
<td>Warnings are highlighted in red and boxed.</td>
</tr>
<tr>
<td></td>
<td>Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.</td>
</tr>
<tr>
<td>We recommended that you use...</td>
<td>Notes are boxed.</td>
</tr>
<tr>
<td></td>
<td>Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the application.</td>
</tr>
<tr>
<td>Example:</td>
<td>Examples are given in blocks on a yellow background titled as &quot;Example&quot;.</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Document conventions
<table>
<thead>
<tr>
<th><strong>Sample Text</strong></th>
<th><strong>Description of Document Convention</strong></th>
</tr>
</thead>
</table>
| *Update* means... The *Databases are out of date* event occurs. | The following semantic elements are italicized in the text:  
  - New terms  
  - Names of application statuses and events |
| Press **ENTER**.  
Press **ALT+F4**. | Names of keyboard keys appear in bold and are capitalized.  
Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously. |
| Click the **Enable** button. | Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold. |
| ➔ **To configure a task schedule**: | The introductory phrases of instructions are italicized and are accompanied by the arrow sign. |
| In the command line, type help. The following message then appears: Specify the date in dd:mm:yy format. | The following types of text content are set off with a special font:  
  - Text in the command line  
  - Text of messages that the application displays on screen  
  - Data that the user must enter. |
| `<User name>` | Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets. |
SOURCES OF INFORMATION ABOUT THE APPLICATION

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

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

IN THIS SECTION

Sources of information to research on your own ................................................................. 9
Discussing Kaspersky Lab applications on the Forum .......................................................... 10
Contacting the Sales Department ....................................................................................... 10
Contacting Technical Writing and Localization Unit by email ............................................ 10

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can use the following sources of information to research on your own:

- Application page at the Kaspersky Lab website
- Application page at the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page 73).

You must have an Internet connection to use the sources of information on the Kaspersky Lab website.

Application page on the Kaspersky Lab website

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

On the web page (http://www.kaspersky.com/kaspersky-pure), you can view general information about the application, its functions, and its features.

The page contains the link to the eStore. There you can purchase or renew the application.

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. The Knowledge Base contains reference articles that are grouped by topic.
On the page of the application in the Knowledge Base (http://support.kaspersky.com/pure), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

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

**Online help**

The online help of the application comprises help files.

Context help contains information about each application window: a listing and description of application settings and related tasks.

Full help provides detailed information about managing computer protection, configuring the application and solving typical user tasks.

**Documentation**

The Kaspersky PURE user guide provides information about how to install, activate, configure, and use the application. The document also describes the application interface and suggests ways for solving typical user tasks while working with the application.

**DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM**

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

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

**CONTACTING THE SALES DEPARTMENT**

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

- By calling our central office in Moscow by phone (http://www.kaspersky.com/contacts).
- By sending a message with your question to sales@kaspersky.com.

Service is provided in Russian and in English.

**CONTACTING TECHNICAL WRITING AND LOCALIZATION UNIT BY EMAIL**

If you have any questions about the documentation, please contact our Technical Documentation Development Group. For example, if you would like to leave feedback.
KASPERSKY PURE

This section contains a description of the application’s features and brief information on the application’s functions and components. You will learn what items are included in the distribution kit and what services are available for registered users of the application. This section provides information about software and hardware requirements that a computer should meet to allow a user to install the application on it.

In this section:

- What’s new
- Main functions and applications
- Distribution kit
- Service for users
- Hardware and software requirements

What’s new

Kaspersky PURE provides the following new features:

- Safe Money has been added to ensure a safe use of online banking services and payment systems, as well as to simplify online shopping (see page 44).

- Improved protection against keyloggers of identity data that you enter on websites:
  - Protection of data input from the computer keyboard has been added (see page 48).
  - The application automatically adds the Virtual Keyboard launch button to password entry fields on websites (see section “Using Virtual Keyboard” on page 46).

- Online storage is now available for storing backup copies of files (see section “Using Online storage” on page 61). This improves the security of data storage and simplifies access to data with the use of cloud technology.

- In order to provide protection against intruders exploiting software vulnerabilities, the feature of protection against exploits has been added to the System Watcher component.

- Password Manager has been improved. The password database can now be stored on remote servers. The sync feature makes your current passwords and identity data available on all your laptops and desktop computers with Kaspersky PURE installed.

- The interface of Kaspersky PURE has been improved with the addition of pop-up tips containing helpful application usage advice.

- The application installation procedure has been simplified (see section “Installing and removing the application” on page 16). The option of automatic installation of the latest version of Kaspersky PURE including a set of the latest updates for the application databases has been added.

- The size of the application databases has been reduced, which allows lowering the size of data to download and speed up the installation of updates.

- The heuristic analysis performed when checking websites for phishing, has been improved.

- The messages shown by Parental Control to children have been adapted. Parental Control accuracy has been improved: this component now uses cloud technology when scanning websites for unwanted content.
**MAIN FUNCTIONS AND APPLICATIONS**

Kaspersky PURE provides comprehensive computer protection. Comprehensive protection means computer protection, data protection and user protection, as well as remote management of Kaspersky PURE on all network computers. Different functions and protection components are available as part of Kaspersky PURE to deliver comprehensive protection.

**Computer Protection**

*Protection components* are designed to protect the computer against known and new threats, network attacks, fraud, and spam and other unsolicited information. Every type of threat is handled by an individual protection component (see the description of components in this section). Protection components can be enabled or disabled independently of one another, and their settings can be configured.

In addition to the constant protection provided by the security components, we recommend that you regularly 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 protection components, for example, because of a low security level set, or for other reasons.

To keep Kaspersky PURE up to date, you need to update the databases and program modules used by the application.

When the safety of any application raises doubts, they can be run in a *safe environment*.

Certain specific tasks that need to be performed occasionally can be performed with the help of *additional tools and wizards*, such as configuring Microsoft® Internet Explorer® or cleaning up the traces of user activity in the system.

The following protection components stand guard over your computer in real time:

Described below is the logic of operation of protection components in the Kaspersky PURE mode recommended by Kaspersky Lab specialists (with default application settings).

**File Anti-Virus**

File Anti-Virus prevents infection of the computer's file system. The component starts upon startup of the operating system, continuously remains in the computer's RAM, and scans all files being opened, saved, or launched on your computer and all connected drives. Kaspersky PURE intercepts each attempt to access a file and scans the 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. A copy of the file will be saved in Backup, or moved to Quarantine.

**Mail Anti-Virus**

Mail Anti-Virus scans incoming and outgoing email messages on your computer. The email is available to the addressee only if it does not contain dangerous objects.

**Web Anti-Virus**

Web Anti-Virus intercepts and blocks the execution of scripts on websites if they pose a threat. Web Anti-Virus also monitors all web traffic and blocks access to dangerous websites.

**IM Anti-Virus**

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.

**Proactive Defense**

Proactive Defense allows detecting of a new malicious program before it performs its malicious activity. The component's operation is based on monitoring and analyzing the behavior of all applications installed on your computer. Depending on the actions being performed by applications, Kaspersky PURE decides whether an 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.
Application Control

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 specified for each group of applications. These rules manage the applications’ access to various operating system resources.

Firewall

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

Network Monitor

Network Monitor is designed for monitoring network activity in real time.

Network Attack Blocker

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

Anti-Spam

Anti-Spam integrates into the mail client installed on your computer and scans all incoming email messages for spam. All messages containing spam are marked with a special header. You can configure Anti-Spam to handle spam messages in a particular way (for example, delete them automatically or move them to a special folder).

Anti-Phishing

Anti-Phishing checks web addresses against lists of malicious and phishing websites. This component is built into Web Anti-Virus, Anti-Spam, and IM Anti-Virus.

Anti-Banner

Anti-Banner blocks ad banners on websites and in application interfaces.

Safe Money

Safe Money provides protection of confidential data when using online banking services and payment systems, and prevents theft of assets when making online payments.

Data protection

The Backup, Data Encryption and Password Manager features are designed to protect data against loss, unauthorized access or theft.

Backup copying

Data stored on a computer can be lost for different reasons, such as exposure to viruses or unauthorized alteration or removal by another user. To avoid losing important information, you should regularly back up data.

The Backup function 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.

Data 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 data in the encrypted container, you must enter a password.
Password Manager

The majority of online services and resources require users to register and enter login details. For security reasons, it is recommended to use different user accounts on different websites and memorize user logins and passwords without writing them down.

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 you enter the Master Password, Password Manager can automatically fill in the fields of different website login forms. The Master Password lets you manage all of your website accounts.

Parental Control

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

Parental Control allows you to set flexible restrictions on access to web resources and applications for different users depending on their age. It also lets you view statistical reports on controlled user activity.

Home Network Control

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.

Home Network Control 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.

**DISTRIBUTION KIT**

You can purchase the application in one of the following ways:

- **Boxed.** Distributed via stores of our partners.
- **At the online store.** Distributed at online stores of Kaspersky Lab (for example, [http://www.kaspersky.com](http://www.kaspersky.com), section eStore) or via partner companies.

If you purchase the boxed version of the application, the distribution kit contains the following items:

- sealed sleeve with the setup CD, which contains application files and documentation files;
- brief User Guide with an activation code;
- End User License Agreement that stipulates the terms, on which you can use the application.

The content of the distribution kit may differ depending on the region in which the application is distributed.

If you purchase Kaspersky PURE at an online store, you copy the application from the website of the store. Information that is required for activating the application will be sent to you by email after your payment has been received.

For more details on ways of purchasing and the distribution kit, contact the Sales Department by sending a message to sales@kaspersky.com.

**SERVICE FOR USERS**

By purchasing a license for the application, you can benefit from the following services during the entire term of the license:

- updates of the application databases and updates to the software package
- support on issues related to the installation, configuration and use of the application by phone or via email
Notifications about the release of new applications by Kaspersky Lab and of new viruses and virus outbreaks. To use this service, subscribe to news delivery from Kaspersky Lab on the Technical Support website.

Advice on issues related to operating systems and third-party applications and technologies is not provided.

**HARDWARE AND SOFTWARE REQUIREMENTS**

To ensure the functioning of Kaspersky PURE, your computer should meet the following requirements:

**General requirements:**
- 700 MB of free disk space on the hard drive.
- CD / DVD-ROM (for installing Kaspersky PURE from a distribution CD).
- Computer mouse.
- Internet connection (for activating the application and updating databases and application modules).
- Microsoft Internet Explorer 8.0 or later.
- Microsoft Windows® Installer 3.0.

Requirements for the operating systems Microsoft Windows XP Home Edition (Service Pack 3 or higher), Microsoft Windows XP Professional (Service Pack 3 or higher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 or higher):
- Intel® Pentium® 800 MHz 32-bit (x86) / 64-bit (x64) processor or later (or a compatible equivalent).
- 512 MB free RAM.

Requirements for the operating systems Microsoft Windows Vista® Home Basic (Service Pack 2 or higher), Microsoft Windows Vista Home Premium (Service Pack 2 or higher), Microsoft Windows Vista Business (Service Pack 2 or higher), Microsoft Windows Vista Enterprise (Service Pack 2 or higher), Microsoft Windows Vista Ultimate (Service Pack 2 or higher), Microsoft Windows 7 Starter (Service Pack 1 or higher), Microsoft Windows 7 Home Basic (Service Pack 1 or higher), Microsoft Windows 7 Home Premium (Service Pack 1 or higher), Microsoft Windows 7 Professional (Service Pack 1 or higher), Microsoft Windows 7 Ultimate (Service Pack 1 or higher), Microsoft Windows 8, Microsoft Windows 8 Pro, Windows 8 Enterprise or higher (x32 and x64):
- Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) processor or later (or a compatible equivalent).
- 1 GB free RAM (for a 32-bit operating system); 2 GB free RAM (for a 64-bit operating system).

Requirements for netbooks:
- Intel Atom™ 1.6 GHz (Z520) processor or a compatible equivalent.
- 1 GB free RAM.
- Intel GMA950 video adapter with at least 64 MB of memory (or a compatible equivalent).
- A 10.1-inch screen at a minimum.

The application does not support Password Manager under 64-bit operating systems.
INSTALLING AND REMOVING THE APPLICATION

This section contains step-by-step instructions for application installation and removal.

**IN THIS SECTION:**

- Installing the application .......................................................... 16
- Upgrading previous version of Kaspersky PURE .............................. 19
- Removing the application .............................................................. 22

**INSTALLING THE APPLICATION**

Kaspersky PURE will be installed on your computer in an interactive mode using the Setup Wizard.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

If the application is meant to protect more than one computer (with the maximum number of computers defined by the terms of the End User License Agreement), it must be installed identically on all computers.

To install Kaspersky PURE on your computer,

run the setup file (a file with the *.exe extension) from the CD with the product.

To install Kaspersky PURE, you can also use a distribution package downloaded from the Internet. The Setup Wizard displays a few additional installation steps for some of the localization languages at that.

**IN THIS SECTION:**

- Step 1. Finding a newer version of the application .......................... 17
- Step 2. Starting the application installation ..................................... 17
- Step 3. Reviewing the End User License Agreement .......................... 17
- Step 5. Installation ........................................................................... 17
- Step 6. Completing installation ........................................................... 18
- Step 7. Activating the application ...................................................... 18
- Step 8. User registration ................................................................. 19
- Step 9. Completing activation ........................................................... 19
**STEP 1. FINDING A NEWER VERSION OF THE APPLICATION**

Before setup, the Setup Wizard checks the Kaspersky Lab update servers for a newer version of Kaspersky PURE.

If it does not find a newer product version on the Kaspersky Lab update servers, the Setup Wizard for the current version will be started.

If the update servers offer a newer version of Kaspersky PURE, you will see a prompt to download and install it on the computer. It is recommended that you install the new version of the application, because newer versions include more enhancements that allow you to ensure more reliable protection of your computer. If you cancel the new version download, the Setup Wizard for the current version will be started. If you decide to install the newer version, product distribution files will be downloaded to your computer and the Setup Wizard for that new version will be started automatically. For a further description of the installation procedure for the newer version, please refer to its corresponding documentation.

**STEP 2. STARTING THE APPLICATION INSTALLATION**

At this step, the Setup Wizard offers you to install the application.

To proceed with the installation, click the Install button.

**STEP 3. REVIEWING THE END USER LICENSE AGREEMENT**

At this step, you should review the license agreement between you and Kaspersky Lab.

Read the End User License Agreement thoroughly and, if you agree with all of its terms, click the Accept button. The application installation will go on.

If the End User License Agreement is not accepted, the application will not be installed.

**STEP 4. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT**

At this step, the Setup Wizard invites you to participate in Kaspersky Security Network. Participation in the program involves sending information about new threats detected on your computer, running applications, and downloaded signed applications to Kaspersky Lab, along with your system information. No private data received from you is collected, processed, or stored.

Review the Kaspersky Security Network Data Collection Statement. If you agree with all of the terms of the Agreement, select the "I want to participate in Kaspersky Security Network (KSN)" check box in the Wizard window.

Click the Next button to proceed with the Wizard installation.

**STEP 5. INSTALLATION**

Installation of the application can take some time. Wait for it to finish.

Once the installation is complete, the Wizard will proceed automatically to the next step.
Kaspersky PURE performs several checks during installation. Those checks may result in detection of the following problems:

- **Non-compliance of the operating system to the software requirements.** During installation the Wizard checks the following conditions:
  - Whether the operating system and the Service Packs meet the software requirements
  - Whether all of the required applications are available
  - Whether the amount of free disk space is enough for installation

If any of the above-listed requirements is not met, the corresponding notification will be displayed on the screen.

- **Presence of incompatible applications on the computer.** If such applications are detected, their list is shown and the user is offered to remove them. Applications that Kaspersky PURE cannot remove automatically should be removed manually. When removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky PURE will continue automatically.

- **Presence of malware on the computer.** If any malicious applications that interfere with installation of anti-virus software are detected on the computer, the Setup Wizard prompts you to download a dedicated tool designed to neutralize infection and named Kaspersky Virus Removal Tool.

If you agree to install the utility tool, the Setup Wizard downloads it from Kaspersky Lab servers, after which installation of the utility starts automatically. If the Wizard cannot download the utility, you will be prompted to download it on your own by clicking the link provided.

### STEP 6. COMPLETING INSTALLATION

At this step, the Wizard informs you of the completion of the application installation. To run Kaspersky PURE immediately, make sure that the Run Kaspersky PURE 3.0 check box is selected and click the Finish button.

In some cases, you may need to reboot your operating system to complete installation. If the Run Kaspersky PURE 3.0 check box is selected, the application is launched automatically after the operating system is rebooted.

If you have cleared the Run Kaspersky PURE 3.0 check box before closing the Wizard, you will have to start the application manually.

### STEP 7. ACTIVATING THE APPLICATION

At this step, the Setup Wizard offers you to activate the application.

*Activation* is a process of putting into operation a full-functional version of the application for a certain period of time.

You will need an Internet connection to activate the application.

You will be offered the following options for Kaspersky PURE activation:

- **Activate commercial version.** Select this option and enter the activation code (see section "About the activation code" on page 26) if you have purchased a commercial version of the application.

- **Activate trial version.** 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 able to use the fully-functional version of the application for the duration of the trial license. When the license expires, trial version cannot be activated for a second time.
**STEP 8. USER REGISTRATION**

This step is only available when activating the commercial version of the application. When activating the trial version, this step is skipped.

Registered users are able to send requests to the Technical Support Service and Virus Lab through My Kaspersky Account on the Kaspersky Lab website, manage activation codes conveniently, and receive the latest information about new products and special offers.

If you agree to register, specify your registration data in the corresponding fields and click the **Next** button to send the data to Kaspersky Lab.

**STEP 9. COMPLETING ACTIVATION**

The Wizard informs you that Kaspersky PURE has been successfully activated. In addition, information about the current license is provided in this window: license type (commercial or trial), expiration date, and number of hosts covered by the license.

If you are using a subscription, information about the subscription status is displayed instead of the license expiration date.

Click the **Finish** button to close the Wizard.

**UPGRADING PREVIOUS VERSION OF KASPERSKY PURE**

If you have a previous version of PURE installed on your computer, you need to upgrade the application to the new version of PURE. If you have a current license for Kaspersky PURE, you will not have to activate the application: the Setup Wizard will automatically retrieve the information about your license for Kaspersky PURE and apply it in the course of the installation process.

Kaspersky PURE will be installed on your computer in an interactive mode using the Setup Wizard.

The Wizard consists of a series of screens (steps) navigated using the **Back** and **Next** buttons. To close the Wizard once it has completed its task, click the **Finish** button. To stop the Wizard at any stage, click the **Cancel** button.

If the application is meant to protect more than one computer (with the maximum number of computers defined by the terms of the End User License Agreement), it must be installed identically on all computers.

> To install Kaspersky PURE on your computer,

run the setup file (a file with the *.exe extension) from the CD with the product.

To install Kaspersky PURE, you can also use a distribution package downloaded from the Internet. The Setup Wizard displays a few additional installation steps for some of the localization languages at that.

**IN THIS SECTION:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Finding a newer version of the application</td>
<td>20</td>
</tr>
<tr>
<td>Step 2</td>
<td>Starting the application installation</td>
<td>20</td>
</tr>
<tr>
<td>Step 3</td>
<td>Reviewing the End User License Agreement</td>
<td>20</td>
</tr>
<tr>
<td>Step 4</td>
<td>Kaspersky Security Network Data Collection Statement</td>
<td>20</td>
</tr>
<tr>
<td>Step 5</td>
<td>Installation</td>
<td>20</td>
</tr>
<tr>
<td>Step 6</td>
<td>Completing installation</td>
<td>21</td>
</tr>
</tbody>
</table>
**STEP 1. FINDING A NEWER VERSION OF THE APPLICATION**

Before setup, the Setup Wizard checks the Kaspersky Lab update servers for a newer version of Kaspersky PURE.

If it does not find a newer product version on the Kaspersky Lab update servers, the Setup Wizard for the current version will be started.

If the update servers offer a newer version of Kaspersky PURE, you will see a prompt to download and install it on the computer. It is recommended that you install the new version of the application, because newer versions include more enhancements that allow you to ensure more reliable protection of your computer. If you cancel the new version download, the Setup Wizard for the current version will be started. If you decide to install the newer version, product distribution files will be downloaded to your computer and the Setup Wizard for that new version will be started automatically. For a further description of the installation procedure for the newer version, please refer to its corresponding documentation.

**STEP 2. STARTING THE APPLICATION INSTALLATION**

At this step, the Setup Wizard offers you to install the application.

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

Depending on the installation type and the localization language, at this step the Wizard offers you to view the License Agreement concluded between you and Kaspersky Lab, also offering you to participate in Kaspersky Security Network.

**STEP 3. REVIEWING THE END USER LICENSE AGREEMENT**

At this step, you should review the license agreement between you and Kaspersky Lab.

Read the End User License Agreement thoroughly and, if you agree with all of its terms, click the **Accept** button. The application installation will go on.

If the End User License Agreement is not accepted, the application will not be installed.

**STEP 4. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT**

At this step, the Setup Wizard invites you to participate in Kaspersky Security Network. Participation in the program involves sending information about new threats detected on your computer, running applications, and downloaded signed applications to Kaspersky Lab, along with your system information. No private data received from you is collected, processed, or stored.

Review the Kaspersky Security Network Data Collection Statement. If you agree with all of the terms of the Agreement, select the "I want to participate in Kaspersky Security Network (KSN)" check box in the Wizard window.

Click the **Next** button to proceed with the Wizard installation.

**STEP 5. INSTALLATION**

Installation of the application can take some time. Wait for it to finish.

Once the installation is complete, the Wizard will proceed automatically to the next step.
Kaspersky PURE performs several checks during installation. Those checks may result in detection of the following problems:

- **Non-compliance of the operating system to the software requirements.** During installation the Wizard checks the following conditions:
  - Whether the operating system and the Service Packs meet the software requirements
  - Whether all of the required applications are available
  - Whether the amount of free disk space is enough for installation

  If any of the above-listed requirements is not met, the corresponding notification will be displayed on the screen.

- **Presence of incompatible applications on the computer.** If such applications are detected, their list is shown and the user is offered to remove them. Applications that Kaspersky PURE cannot remove automatically should be removed manually. When removing incompatible applications, you will need to reboot your operating system, after which installation of Kaspersky PURE will continue automatically.

- **Presence of malware on the computer.** If any malicious applications that interfere with installation of anti-virus software are detected on the computer, the Setup Wizard prompts you to download a dedicated tool designed to neutralize infection and named *Kaspersky Virus Removal Tool*.

  If you agree to install the utility tool, the Setup Wizard downloads it from Kaspersky Lab servers, after which installation of the utility starts automatically. If the Wizard cannot download the utility, you will be prompted to download it on your own by clicking the link provided.

**STEP 6. COMPLETING INSTALLATION**

This window of the Wizard informs you of the successful completion of the application installation.

Restart the operating system after the application has been installed.

If the Run Kaspersky PURE 3.0 check box is selected, the application will be run automatically after you reboot your operating system.

If you have cleared the Run Kaspersky PURE 3.0 check box before closing the Wizard, you will need to run the application manually.
Removing the Application

After uninstalling Kaspersky PURE, your computer and personal data will be unprotected!

Kaspersky PURE is uninstalled by means of the Setup Wizard.

To run the wizard,

In the Start menu select Programs → Kaspersky PURE 3.0 → Remove Kaspersky PURE 3.0.

In this section:

Step 1. Saving data for future use ................................................................. 22
Step 2. Confirm removal ................................................................................. 23
Step 3. Removing the application. Completing removal ..................................... 23

Step 1. Saving data for future use

At this stage you can specify which application data has to be saved for future use during subsequent installation of the application (for example, its new version).

You can specify the following data types for future use:

- **License information** – a set of data that rules out the need to activate the new application by allowing you to use it under the current license unless the license expires before you start the installation.

- **Quarantine objects** – files that are scanned by the application and placed in Backup or to Quarantine.

    After Kaspersky PURE is removed from the computer, quarantined files become unavailable. You should install Kaspersky PURE to handle those files.

- **Application operating settings** – values of the application settings selected during configuration.

    Kaspersky Lab does not guarantee support of previous application version settings. After the new version is installed, we recommend checking the correctness of its settings.

- **iChecker data** are files that contain information about objects that have already been scanned with iChecker technology.

- **Encrypted containers (including the data)** – files moved to encrypted containers using the Data Encryption feature.

- **Password Manager databases (for all users)** – user accounts, personal notes, bookmarks, and business cards created using the Password Manager feature.

- **Anti-Spam databases** are databases that contain samples of spam messages downloaded and saved by the application.

By default, the application prompts you to save information about activation.
To save data for future use

select the check boxes for the data types you want to save.

**STEP 2. CONFIRM REMOVAL**

Because application removal jeopardizes the safety of the computer and personal data, the user is required to confirm the intention to remove the application. Click the **Delete** button to do so.

**STEP 3. REMOVING THE APPLICATION. COMPLETING REMOVAL**

At this stage, the Setup Wizard removes the application from the computer. Wait for the removal process to finish.

When removing the application, you must reboot your operating system. If you cancel immediate reboot, completion of the removal procedure will be postponed until the operating system is rebooted or the computer is turned off and then restarted.
APPLICATION LICENSING

This section contains information about the basic concepts of application activation. Read this section to learn more about the purpose of the End User License Agreement, license types, ways of activating the application, and the license renewal.

IN THIS SECTION:

About the End User License Agreement ......................................................................................................................... 24
About the license ................................................................................................................................................................... 24
About data provision ............................................................................................................................................................. 25
About the activation code ...................................................................................................................................................... 26

ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

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

It is deemed that you accept the terms of the License Agreement by confirming that you agree with the License Agreement when installing the application. If you do not accept the terms of the License Agreement, you must abort installation or refrain from using the application.

ABOUT THE LICENSE

A license is a time-limited right to use the application, granted under the End User License Agreement. The license stipulates a unique activation code for your copy of Kaspersky PURE.

A current license entitles you to the following kinds of services:

- The right to use the application on one or several devices.
  The number of devices on which you may use the application is specified in the End User License Agreement.

- Assistance from Kaspersky Lab Technical Support.

- Other services available from Kaspersky Lab or its partners during the term of the license (see the section “Service for users” on page 14).

The scope of services and application usage term depend on the type of license under which the application is activated.

The following license types are possible:

- Trial – a free license intended for trying out the application.
  Trial license usually has a short term. As soon as the license expires, all Kaspersky PURE features are disabled. To continue using the application, you need to purchase a commercial license.
• **Commercial** – a paid license offered upon purchase of the application.

When the commercial license expires, the application continues running though with a limited functionality (for example, updating and using Kaspersky Security Network are not available). You still can benefit all of the application components and perform scans for viruses and other malware, but using only the databases that had been installed last before the license expired. To continue using Kaspersky PURE in fully functional mode, you must renew your commercial license.

We recommend renewing the license before its expiration to ensure maximum protection of your computer against all security threats.

## ABOUT DATA PROVISION

To increase the protection level, by accepting the provisions of the License Agreement, you agree to provide the following information to Kaspersky Lab in automatic mode:

- information about the checksums of processed files (MD5);
- information required for assessing the reputations of URLs;
- statistics of the use of product notifications;
- statistical data for protection against spam;
- data on Kaspersky PURE activation and version currently in use;
- information about the types of detected threats;
- information about digital certificates being currently in use and information required to verify them.

If the computer is equipped with TPM (Trusted Platform Module), you also agree to provide Kaspersky Lab the TPM report on the operating system’s booting and information required to verify it. If an error occurs during Kaspersky PURE installation, you agree to automatically supply Kaspersky Lab with information about the error code, installation package currently in use, and your computer.

When you participate in Kaspersky Security Network, the following information generated during Kaspersky PURE operation is automatically relayed to Kaspersky Lab:

- information about the hardware and software installed on the computer;
- information about the anti-virus protection status of the computer, as well as all potentially malicious objects and actions, and decisions made in relation to those objects and actions;
- information about applications being downloaded and run;
- information about interface errors and usage of the Kaspersky PURE interface;
- information about the version of the databases being currently in use;
- statistics of updates and connections to Kaspersky Lab servers;
- statistics of the actual time spent by application components on the scanning of objects.

Also, additional checking at Kaspersky Lab may require sending files (or parts of files) that are imposed to an increased risk of being exploited by intruders to do harm to the user’s computer or data.

Kaspersky Lab protects any information received in this way as prescribed by the law. Kaspersky Lab uses any retrieved information as general statistics only. General statistics are automatically generated using original retrieved information and do not contain any private data or other confidential information. Original retrieved information is stored in encrypted form; it is cleared as it is accumulated (twice per year). General statistics are stored indefinitely.
ABOUT THE ACTIVATION CODE

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

The activation code is a unique sequence of twenty digits and Latin letters in the format xxxxx-xxxxx-xxxxx-xxxxx.

Depending on how you purchased the application, you can obtain the activation code in one of the following ways:

- When you buy a boxed version of Kaspersky PURE, the activation code is provided in the manual or on the retail box that contains the installation CD.
- When you buy Kaspersky PURE from an online store, the activation code is emailed to the address that you specify when ordering.

The license term countdown starts from the date when you activate the application. If you have purchased a license entitling to the use of Kaspersky PURE on several devices, the term of the license starts counting down from the moment you have first applied the activation code.

If you have lost or accidentally deleted your activation code after the activation, contact Kaspersky Lab Technical Support to restore it.
# PERFORMING COMMON TASKS

This section contains step-by-step instructions for performing typical user tasks that the application provides.

## In this section:

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating the application</td>
<td>28</td>
</tr>
<tr>
<td>Purchasing and renewing a license</td>
<td>28</td>
</tr>
<tr>
<td>Managing application notifications</td>
<td>29</td>
</tr>
<tr>
<td>Assessing the computer protection status and resolving security issues</td>
<td>30</td>
</tr>
<tr>
<td>Updating databases and application software modules</td>
<td>31</td>
</tr>
<tr>
<td>Scanning critical areas of your computer for viruses</td>
<td>32</td>
</tr>
<tr>
<td>Full scan of the computer for viruses</td>
<td>32</td>
</tr>
<tr>
<td>Scanning a file, folder, disk, or another object for viruses</td>
<td>33</td>
</tr>
<tr>
<td>Scanning the computer for vulnerabilities</td>
<td>34</td>
</tr>
<tr>
<td>Restoring a file deleted or disinfect ed by the application</td>
<td>34</td>
</tr>
<tr>
<td>Recovering the operating system after infection</td>
<td>36</td>
</tr>
<tr>
<td>Blocking unwanted email (spam)</td>
<td>38</td>
</tr>
<tr>
<td>Scanning email and filtering attachments in email messages</td>
<td>38</td>
</tr>
<tr>
<td>Assessing the safety status of a website</td>
<td>39</td>
</tr>
<tr>
<td>Blocking access to websites of various regions</td>
<td>40</td>
</tr>
<tr>
<td>Remote management of home network protection</td>
<td>40</td>
</tr>
<tr>
<td>Handling unknown applications</td>
<td>41</td>
</tr>
<tr>
<td>Protecting privacy data against theft</td>
<td>43</td>
</tr>
<tr>
<td>Backup copying</td>
<td>59</td>
</tr>
<tr>
<td>Password-protecting access to Kaspersky PURE settings</td>
<td>62</td>
</tr>
<tr>
<td>Using Parental Control</td>
<td>63</td>
</tr>
<tr>
<td>Pausing and resuming computer protection</td>
<td>65</td>
</tr>
<tr>
<td>Viewing computer protection report</td>
<td>66</td>
</tr>
<tr>
<td>Restoring the default application settings</td>
<td>66</td>
</tr>
<tr>
<td>Importing the application settings to Kaspersky PURE installed on another computer</td>
<td>69</td>
</tr>
<tr>
<td>Creating and using a Rescue Disk</td>
<td>69</td>
</tr>
</tbody>
</table>
ACTIVATING THE APPLICATION

You need to activate the application to be able to use its functionality and associated services.

If you did not activate the application during installation, you can do so later. You will be reminded about the need to activate the application by Kaspersky PURE messages appearing in the taskbar notification area. Kaspersky PURE is activated using the Activation Wizard.

To run the Kaspersky PURE activation wizard, perform one of the following:

- Click the Activate link in the Kaspersky PURE notification window that appears in the taskbar notification area.
- In the lower part of the main application window, click the License link. In the Licensing window that opens, click the Activate the application button.

When working with the Application Activation Wizard, you should specify values for a collection of settings.

Step 1. Entering the activation code

Enter the activation code (see section "About the activation code" on page 26) in the corresponding field and click the Next button.

Step 2. Requesting activation

If the activation request is sent successfully, the Wizard automatically proceeds to the next step.

Step 3. Entry of registration data

Registered users are permitted to use the following features:

- Send requests to Technical Support Service and Anti-Virus Lab from My Kaspersky Account on the website of Kaspersky Lab.
- Manage activation codes.
- Receive information about new products and special offers from Kaspersky Lab.

Specify your registration details and click the Next button.

Step 4. Activating the application

If the application activation has been successful, the Wizard automatically proceeds to the next window.

Step 5. Wizard completion

This Wizard window shows information about the activation results.

Click the Finish button to close the Wizard.

PURCHASING AND RENEWING A LICENSE

If you have installed Kaspersky PURE without a commercial license, you can purchase one after installation. On acquiring a commercial license, you will receive an activation code that you have to use to activate the application (see section "Activating the application" on page 28).
When your license expires, you can renew it. You can do so by specifying a new activation code without waiting for the current license to expire. When the current license expires, Kaspersky PURE will be automatically activated by means of the reserve activation code.

To purchase a license:

1. Open the main application window.
2. Click the License link in the bottom part of the main window to open the Licensing window.
3. In the window that opens, click the Buy activation code button.
   The eStore web page opens where you can purchase a license.

To enter a new activation code:

1. Open the main application window.
2. Click the License link in the bottom part of the main window to open the Licensing window.
3. In the window that opens, click the Activate the application button.
   The Application Activation Wizard opens.
4. Enter the activation code in the corresponding fields and click the Next button.
   Kaspersky PURE then sends the data to the activation server for verification. If the verification is successful, the Activation Wizard automatically proceeds to the next step.
5. When the Wizard sequence has ended, click the Finish button.

Managing application notifications

Notifications that appear in the taskbar notification area inform you of events occurring in the application's operation and requiring your attention. Depending on how critical the event is, you may receive the following types of notification:

- **Critical notifications** – inform you of events that have a critical importance for the computer's security, such as detection of a malicious object or a dangerous activity in the system. Windows of critical notifications and pop-up messages are red-colored.

- **Important notifications** – inform you of events that are potentially important for the computer's security, such as detection of a probably infected object or a suspicious activity in the system. Windows of important notifications and pop-up messages are yellow-colored.

- **Information notifications** – inform you of events that do not have critical importance for the computer's security. Windows of information notifications and pop-up messages are green-colored.

If a notification is displayed on the screen, you should select one of the options that are suggested in the notification. The optimal option is the one recommended as the default by Kaspersky Lab experts.
ASSESSING THE COMPUTER PROTECTION STATUS AND RESOLVING SECURITY ISSUES

Problems with computer protection are signaled by the color of the Kaspersky PURE main window (see figure below). The indicator changes color depending on the host protection status: the green indicator means that the computer is protected; the yellow one indicates protection-related problems, and the red one signals a serious threat to computer security. You are advised to fix the security problems and neutralize threats immediately.

Figure 1. Red color indication of the main window
The **Fix** button (see figure above) is shown on the protection status indicator in the upper right part of the main application window when computer security problems are present. Clicking the **Fix** button opens the **Security Problems** window (see figure below), which contains detailed information about the status of computer protection and ways to fix security problems and neutralize threats.

![Security Problems window](image)

**Figure 2. Security Problems window**

Protection-related problems are grouped by categories. For each problem, actions are listed that you can use to solve the problem.

You can use Home Network Control to check the status of protection on other home network computers (see section "Remote management of home network protection" on page 40).

## Updating databases and application modules

By default, Kaspersky PURE automatically checks for updates on the Kaspersky Lab update servers. If the server stores a set of recent updates, Kaspersky PURE downloads and installs them in background mode. You can run a Kaspersky PURE update manually at any time from the main application window or the context menu of the application icon in the taskbar notification area.

An Internet connection is required to download updates from Kaspersky Lab servers.

- To run an update from the context menu of the application icon in the taskbar notification area,

  in the context menu of the application icon, select the **Update** item.
To run an update from the main application window:

1. Open the main application window.
2. Click the Update link in the Computer Protection section to run the database update.

Scanning Critical Areas of Your Computer for Viruses

A Critical Areas Scan involves scanning the following objects:

- objects loaded upon system startup
- system memory
- boot sectors of the disk.

To start a Critical Areas Scan from the main application window:

1. Open the main application window and click the Computer Protection button.
2. In the left part of the window that opens, select the Scan section.
3. In the Critical Areas Scan section in the right part of the window, click the button.

Full Scan of the Computer for Viruses

During a full scan, Kaspersky PURE scans the following objects by default:

- system memory;
- objects loaded upon system startup
- system backup
- hard drives and removable drives.

We recommend running a full scan immediately after installing Kaspersky PURE on the computer.

To start a full scan from the main application window:

1. Open the main application window.
2. Click the Scan link in the Computer Protection section to open the list of scan tasks.
3. Click the Full Scan link to run a full scan.
SCANNING A FILE, FOLDER, DISK, OR ANOTHER OBJECT FOR VIRUSES

You can use the following methods to scan an object for viruses:

- from the context menu of the object;
- from the main application window

**To start a virus scan from the object context menu:**

1. Open Microsoft Windows Explorer and go to the folder which contains the object to be scanned.
2. Right-click to open the context menu of the object (see the figure below) and select **Scan for viruses**.

![Context menu of an executable file](image)

**To start scanning an object from the main application window:**

1. Open the main application window and click the **Computer Protection** button.
2. In the left part of the window that opens, select the **Scan** section.
3. Specify the object to be scanned in one of the following ways:
   - Click the **specify** link in the bottom right part of the window to open the **Custom Scan** window and select check boxes opposite the folders and disks that need to be scanned.
   
   If the window does not list an object that needs to be scanned, perform the following:

   a. Click the **Add** link in the bottom left part of the window to open the **Select object to scan** window.
b. In the **Select object to scan** window that opens, select an object to be scanned.

- Drag an object to scan into the dedicated area of the main window (see figure below).

![Drag and drop objects for a custom scan](image)

*Figure 4. An area of the Scan window, into which you should drag an object to scan*

## Scanning the Computer for Vulnerabilities

**Vulnerabilities** are unprotected portions of software code which intruders may deliberately use for their purposes, for example, to copy data used in unprotected applications. Scanning your computer for vulnerabilities helps you to reveal any such weak points in your computer. You are advised to remove the detected vulnerabilities.

- **To start a vulnerability scan from the main application window:**
  1. Open the main application window and click the **Computer Protection** button.
  2. In the left part of the window that opens, select the **Scan** section.
  3. In the window that opens in the **Vulnerability Scan** section, click the **button.

## Restoring a File Deleted or Disinfected by the Application

Kaspersky Lab recommends that you avoid restoring deleted and disinfected files, as they may pose a threat to your computer.

To restore a deleted or disinfected file, you can use its backup copy created by the application during a scan of the file.

- **To restore a file that has been deleted or disinfected by the application:**
  1. Open the main application window and click the **Computer Protection** button.
2. In the left part of the window that opens, click the **Quarantine: <number of files>** link (see figure below).

![Computer Protection window](image)

*Figure 5. Computer Protection window*
3. In the **Quarantine** window that opens, select the required file from the list and click the **Restore** button (see figure below).

Kaspersky PURE restores the specified file to the folder that used to store the file that has been removed and disinfected by the application.

![Figure 6. Quarantine window](image)

**RECOVERING THE OPERATING SYSTEM AFTER INFECTION**

If you suspect the operating system of your computer to be corrupted or modified due to malware activity or a system failure, use the *post-infection Microsoft Windows troubleshooting wizard* that clears the system of any traces of malicious objects. Kaspersky Lab recommends that you run the Wizard after the computer has been disinfected to make sure that all threats and damage caused by infections have been fixed.

The Wizard checks whether there are any changes to the system, such as the following: access to the network being blocked, known file format extensions have been changed, the toolbar is locked, etc. There are different reasons for these different kinds of damage. These reasons may include the activity of malicious programs, incorrect system configuration, 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 that requires immediate attention. Based on the review, a list of actions necessary to eliminate the problems is generated. The Wizard groups these actions by category based on the severity of the problems detected.
To start the Microsoft Windows Troubleshooting Wizard:

1. Open the main application window.
2. In the bottom part of the window, select the Additional Tools section.
3. In the window that opens, in the Post-infection Microsoft Windows troubleshooting section, click the Run button.

The Microsoft Windows Troubleshooting Wizard window opens.

The Wizard consists of a series of screens (steps) navigated using the Back and Next buttons. To close the Wizard once it has completed its task, click the Finish button. To stop the Wizard at any stage, click the Cancel button.

Let us examine the Wizard steps in detail.

**Step 1. Starting Microsoft Windows Troubleshooting**

Make sure that the Wizard option Search for problems caused by malware activity is selected and click the Next button.

**Step 2. Problems search**

The Wizard will search for problems and damage in need of repair. Once the search is complete, the Wizard will proceed to the next step automatically.

**Step 3. Selecting troubleshooting actions**

All damage found during the previous step is grouped based on the type of danger it poses. For each group of damage, Kaspersky Lab recommends a sequence of actions to repair the damage. There are three groups of actions:

- **Strongly recommended actions** eliminate problems posing a serious security threat. You are advised to perform all actions of this group.
- **Recommended actions** eliminate problems that present a potential threat. You are advised to perform all actions of this group too.
- **Additional actions** repair system damage which does not pose a current threat, but may pose a danger to the computer’s security in the future.

To view the actions within a group, click the + icon to the left of the group name. To make the Wizard perform a certain action, select the check box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, clear the box next to it.

It is strongly recommended not to clear the checkboxes selected by default because doing so will leave your computer vulnerable to threats.

Having defined the set of actions which the Wizard will perform, click the Next button.

**Step 4. Eliminating problems**

The Wizard will perform the actions selected during the previous step. The elimination of problems may take some time. Once the troubleshooting is complete, the Wizard will automatically proceed to the next step.
Step 5. Wizard completion
Click the Finish button to close the Wizard.

Blocking unwanted email (spam)
If you receive large quantities of unsolicited email (spam), enable the Anti-Spam component and set the recommended security level.

To enable Anti-Spam and set the recommended security level:
1. Open the main application window.
2. In the top part of the window, click the Settings link.
3. In the left part of the window, in the Protection section, select the Anti-Spam component.
4. Select the Enable Anti-Spam check box in the right part of the window.
5. Make sure the security level in the Security level section is set to Recommended.
   If the security level is set to Low or Custom, click the Default button. The security level will automatically be set to Recommended.

Scanning email and filtering attachments in email messages
Kaspersky PURE allows scanning email messages for dangerous objects using Mail Anti-Virus. Mail Anti-Virus starts when the operating system launches and remains in the RAM permanently, scanning all email messages that are sent or received over POP3, SMTP, IMAP, MAPI, and NNTP, as well as via encrypted connections (SSL) over POP3, SMTP and IMAP.

By default, Mail Anti-Virus scans both incoming and outgoing email. If necessary, you can enable scanning of incoming email only.

To scan only incoming email messages:
1. Open the main application window.
2. In the top part of the window, click the Settings link.
3. In the left part of the window, in the Protection Center section, select the Mail Anti-Virus component.
4. Click the Settings button in the right part of the window.
   The Mail Anti-Virus window opens.
5. In the window that opens, use the General tab in the Protection scope section to select the Incoming messages only option.
   If no threats have been detected in an email message, or if all infected objects have been successfully disinfected, the message becomes available for further operations. If the component fails to disinfect an infected object, Mail Anti-Virus renames or deletes the object from the message and expands the message subject with a notification stating that the message has been processed by Kaspersky PURE. Before deleting an object, Kaspersky PURE creates a backup copy of it and places this copy to Quarantine.

Malicious programs may spread in the form of attachments in email messages. You can enable filtering of attachments in email messages. Filtering allows automatically renaming or deleting attached files of types that you have specified.
To enable attachment filtering in email messages:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the left part of the window, in the **Protection Center** section, select the **Mail Anti-Virus** component.
4. Click the **Settings** button in the right part of the window.
   
   The **Mail Anti-Virus** window opens.
5. In the window that opens, on the **Attachment filter** tab select an attachment filtering mode (**Rename selected attachment types** or **Delete selected attachment types**).
6. From the list of file types (extensions) select attachment types that should be filtered.
   
   If you want to add a mask of a new file type:
   a. Click the **Add** link in the bottom part of the window to open the **Input file name mask** window.
   b. In the window that opens, enter a file type mask.
7. Click the **Apply** button in the **Settings** window.

**Assessing the Safety Status of a Website**

Kaspersky PURE allows checking a website for security before going to the website by a link. To do this, a module named **Kaspersky URL Advisor** is used.

Kaspersky URL Advisor is not available in Metro-style Microsoft Internet Explorer 10, as well as in Microsoft Internet Explorer 10, if the **Enhanced Protected Mode** check box is selected in the browser settings.

Kaspersky URL Advisor is integrated into Microsoft Internet Explorer, Google Chrome™, and Mozilla™ Firefox™ browsers, checking links on web pages opened in the browser. Kaspersky PURE displays one of the following icons next to each link:

- 🏛️ – if the web page opened by clicking the link is safe according to Kaspersky Lab
- 🚫 – if there is no information about the safety status of the web page opened by clicking the link
- 🎥 – if the web page opened by clicking the link is dangerous according to Kaspersky Lab.

When rolling the mouse pointer over an icon, a pop-up window with more details on the link is displayed.

By default, Kaspersky PURE checks links in search results only. You can enable link checking on every website.

To enable link checking on every website:

1. Open the main application window.
2. In the top part of the window, click the **Settings** link.
3. In the **Settings** window that opens, go to the **Protection Center** section, select the **Web Anti-Virus** subsection and click the **Settings** button.

The **Web Anti-Virus** window opens.
4. In the window that opens, on the Safe Surf tab, in the Kaspersky URL Advisor section click the Settings button. The Kaspersky URL Advisor settings window opens.

5. In the window that opens, in the Scan mode section select All URLs.

6. Click the Apply button in the Settings window.

BLOCKING ACCESS TO WEBSITES OF VARIOUS REGIONS

According to statistics collected by Kaspersky Lab, the infection rates of websites may vary depending on the country of origin. Kaspersky PURE uses a component named Geo Filter to block access to websites that belong to specified regional domains with high infection rates.

When Geo Filter is enabled, Kaspersky PURE allows or blocks access to a regional domain, or requests access permission from you, depending on your choice.

To enable and configure Geo Filter:

1. Open the main application window.

2. In the top part of the window, click the Settings link.

3. In the Settings window that opens, go to the Protection Center section, select the Web Anti-Virus subsection and click the Settings button.

   The Web Anti-Virus window opens.

4. In the window that opens, on the Geo Filter tab select the Enable filtering by regional domains check box.

5. In the bottom part of the window, in the list of controlled domains specify domains to which access should be allowed or blocked, or specify those requiring an access permission request.

6. Click the Apply button in the Settings window.

REMOTE MANAGEMENT OF HOME NETWORK PROTECTION

The Home Network Control functions are designed to control Kaspersky PURE installed on home network computers remotely from the administrator’s workstation.

Home Network Control lets you accomplish the following home network security tasks:

- view the list of security problems on a separate computer on the network and fix some of them remotely
- run virus scans on several computers on the home network simultaneously
- update databases on several computers on the home network simultaneously

To view the list of security problems on a particular computer on the network:

1. Open the main application window and click the Home Network Control button in the lower part of the window.

2. In the upper part of the Home Network Control window that opens, 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 in the Problems section, click the List button.

   The Security Problems window opens, showing information on security problems detected on the selected computer.
To scan several computers on the network for viruses:

1. Open the main application window and click the **Home Network Control** button in the lower part of the window.
   
   The **Home Network Control** window opens.

2. Click the **Scan for viruses** link to open the **Group start of scanning** window.

3. In the **Group start of scanning** window, select the tab with the requisite scan type (**Full Scan** or **Critical Areas Scan**).

4. Select the computers you want to scan and click the **Run scan** button.

To update databases on several network computers simultaneously:

1. Open the main application window and click the **Home Network Control** button in the lower part of the window.
   
   The **Home Network Control** window opens.

2. Click the **Update databases** link to open the **Group start of update** window.

3. In the **Group start of update** window, select the computers on which you want the databases updated and click the **Run update** button.

**Handling unknown applications**

Kaspersky PURE helps to minimize the risk involved in using unknown applications (such as the risk of infection with viruses and unwanted changes to operating system settings).

Kaspersky PURE includes components and tools for checking the reputation of an application and launching it in Safe Run mode, which isolates it from the operating system.

**Controlling application activities on the computer and on the network**

Application Control prevents applications from performing actions that may be dangerous for the system and ensures control of access to operating system resources and your identity data.

The component tracks actions performed in the system by applications installed on the computer and regulates them based on the Application Control rules. These rules regulate activity affecting computer security, including applications' access to protected resources, such as files and folders, registry keys, and network addresses.

Applications' network activity is controlled by the Firewall component.

When an application is first run on the computer, Application Control checks it for safety and moves to one of the groups (Trusted, Untrusted, High Restricted, or Low Restricted). The group defines the rules that Kaspersky PURE should apply for controlling the activity of this application.

You can edit application control rules manually.

To edit application rules manually:

1. Open the main application window.

2. In the top part of the window, click the **Settings** link.

3. In the **Settings** window that opens, select the **Application Control** subsection in the **Protection Center** section.
4. In the right part of the window, in the **Configure application rules, protect digital identity data and other resources** section, click the **Applications** button.

5. In the **Applications** window that opens, select the desired application from the list and click the **Edit** button.

6. In the **Application rules** window that opens, set the application rules:
   - To configure rules of access to operating system resources for an application:
     a. On the **Files and system registry** tab select the required resource category.
     b. Right-click the column with an available action on the resource (Read, Write, Delete, or Create) to open the context menu and select the required value from it (Allow, Block, or Prompt for action).
   - To configure the rights of an application to perform various actions in the operating system:
     a. On the **Rights** tab select the required category of rights.
     b. Right-click the **Permission** column to open the context menu and select the required value from it (Allow, Block, or Prompt for action).
   - To configure the rights of an application to perform various actions on the network:
     a. On the **Network rules** tab click the **Add** button.
     b. In the window that opens, specify the required rule settings and click the **OK** button.
     c. Assign a priority to the new rule by using the **Move up** and **Move down** buttons to move it up or down the list.
   - To exclude certain actions from the scope of Application Control, on the **Exclusions** tab select the check boxes for actions that should not be controlled.

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

7. Click the **Apply** button in the **Settings** window.

**CHECKING APPLICATION REPUTATION**

Kaspersky PURE allows you to learn the reputation of applications from users all over the world. The reputation of an application includes the following indicators:

- publisher name;
- information about the digital signature (available if a digital signature exists);
- information about the group, in which the application has been included by Application Control or a majority of users of Kaspersky Security Network;
- the number of Kaspersky Security Network users who use the application (available if the application belongs to the Trusted group in the Kaspersky Security Network database);
- time when the application became known in Kaspersky Security Network;
- countries where the application is the most widespread.

Application reputation check is available if you have agreed to participate in Kaspersky Security Network.
To learn the reputation of an application, select **Check reputation in KSN** in the context menu of the executable file of the application (see figure below).

![Context menu of an executable file in Microsoft Windows](image)

A window with information about the reputation of the application in KSN opens.

**PROTECTING PRIVACY DATA AGAINST THEFT**

Kaspersky PURE helps you protect your personal data against theft:

- passwords, user names, and other registration data;
- account numbers and bank cards;
- confidential data.

Kaspersky PURE includes components and tools that allow you to protect your personal data against theft attempts committed by hackers using such methods as phishing and interception of data entered at the keyboard.

Protection of data when using Internet banking services and shopping at online stores is provided by Safe Money features.

Protection against phishing is ensured by Anti-Phishing, implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components.

Protection against interception of data entered at the keyboard is provided by the Virtual Keyboard, Secure keyboard input and Password Manager.

Protection of data against unauthorized access is ensured by the use of Data Encryption.
The Privacy Cleaner Wizard is designed for clearing the computer of all information about the user’s activities.

**In this section:**

- Safe Money ........................................................................................................................................... 44
- Protection against phishing ...................................................................................................................... 45
- Using Virtual Keyboard .......................................................................................................................... 46
- Secure keyboard input ............................................................................................................................ 48
- Password protection ............................................................................................................................... 49
- Data Encryption ...................................................................................................................................... 52
- Unused Data Cleaner ............................................................................................................................... 53
- File Shredder .......................................................................................................................................... 55
- Privacy Cleaner ...................................................................................................................................... 57

**SAFE MONEY**

To provide protection for confidential data that you enter on websites of banks and payment systems (such as banking card numbers, passwords for access to online banking services), as well as to prevent theft of assets when making online payments, Kaspersky PURE offers you to open such websites in Safe Run for Websites.

**Safe Run for Websites** cannot be run if the *Enable Self-Defense* check box is cleared in the *Advanced Settings* section, the *Self-Defense* subsection of the application settings window.

You can configure Safe Money so that the application could automatically recognize websites of banks and payment systems.

Safe Money is not available in the Metro-style Microsoft Internet Explorer 10, as well as in Microsoft Internet Explorer 10, if the *Enhanced Protected Mode* check box is selected in the browser settings. You can Enable Safe Run for Websites mode from the Kaspersky PURE interface.

**To configure Safe Money:**

1. Open the main application window.
2. In the top part of the window, click the *Settings* link.
3. In the *Settings* window that opens, in the *Protection Center* section select the *Safe Money* subsection.
4. Select the *Enable Safe Money* check box.
5. To enable notification of vulnerabilities detected in the operating system before launching Safe Run for Websites, select the *Notify about operating system vulnerabilities* check box.
6. To configure Safe Money for a specified website:
   a. In the *Banks and payment system websites* list click the *Add* button.
      The *Website for Safe Money* window opens.
   b. In the window that opens, in the *Bank or payment system website* field enter the URL of a website that should be opened in Safe Run for Websites.
The URL of a website should be preceded by https:// protocol prefix that Safe Run for Websites uses by default.

c. If necessary, in the Description field enter the name or a description of that website.

d. Select a method for launching Safe Run for Websites when opening the website:
   • If you want Kaspersky PURE to offer you to launch Safe Run for Websites every time you open the website, select Prompt for action.
   • If you want Kaspersky PURE to open the website in Safe Run for Websites automatically, select Run the protected browser automatically.
   • If you want to disable Safe Money for the website, select Do not run the protected browser.

7. Click the Apply button in the Settings window.

PROTECTION AGAINST PHISHING

Protection against phishing is provided by the Anti-Phishing functionality implemented in the Web Anti-Virus, Anti-Spam, and IM Anti-Virus components. Enable these components to ensure comprehensive protection against phishing.

You can configure additional anti-phishing protection settings in the Web Anti-Virus and IM Anti-Virus components.

To configure anti-phishing protection when Web Anti-Virus is running:

1. Open the main application window.

2. In the top part of the window, click the Settings link.

3. In the Settings window that opens, go to the Protection section, select the Web Anti-Virus subsection and click the Settings button.

   The Web Anti-Virus window opens.

4. In the window that opens, on the General tab, in the Kaspersky URL Advisor section, select the Check web pages for phishing check box.

5. If you want Anti-Phishing to use heuristic analysis click the Additional button when scanning web pages.

   The Anti-Phishing settings window opens.

6. In the window that opens, select the Use Heuristic Analysis to check web pages for phishing and set the scan detail level.

7. Click the Apply button in the Settings window.

To configure anti-phishing protection for use during IM Anti-Virus operation:

1. Open the main application window.

2. In the top part of the window, click the Settings link.

3. In the Settings window that opens, select the IM Anti-Virus subsection in the Protection section.

4. In the right part of the window, in the Scan methods section, select the Check if URLs are listed in the database of phishing URLs check box.

5. Click the Apply button in the Settings window.
**USING VIRTUAL KEYBOARD**

When working on the Internet, you frequently need to enter your personal data or your username and password. For example, this is required when registering on websites, shopping online, or using Internet banking.

There is a risk that this personal information can be intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

The Virtual Keyboard tool prevents the interception of data entered via the keyboard.

Virtual Keyboard only prevents the interception of privacy data when working with Microsoft Internet Explorer, Mozilla Firefox and Google Chrome browsers. When used with other browsers, Virtual Keyboard does not protect personal data being entered against interception.

Virtual Keyboard is not available in the Metro-style Microsoft Internet Explorer 10, as well as in Microsoft Internet Explorer 10, if the Enhanced Protected Mode check box is selected in the browser settings. In this case we recommend using the virtual keyboard from the Kaspersky PURE interface.

Virtual Keyboard cannot protect your personal data if a website that requires entering such data has been hacked, because if it is hacked, the information will be obtained directly by the intruders.

Many programs classified as spyware can take screenshots, which then are automatically transmitted to an intruder for further analysis and for stealing the user’s personal data. Virtual Keyboard prevents the use of screenshots to intercept entered personal data.

The Virtual Keyboard does not prevent making screenshots using **Print Screen** key and other combinations of keys provided by the operating system settings, as well as making screenshots using DirectX.

Virtual Keyboard features:

- Virtual Keyboard keys have to be pressed with the mouse pointer.

- Unlike with the real keyboard, it is impossible to press several Virtual Keyboard keys simultaneously. This is why using key combinations (such as **ALT+F4**) requires pressing the first key (for example, **ALT**), then the second key (for example, **F4**), and then the first key again. Pressing the key again is equivalent to releasing a key on a real keyboard.

- The Virtual Keyboard language can be switched using the same shortcut that is configured in the operating system settings for the physical keyboard. You have to right-click the other key (for example, if the **LEFT ALT-SHIFT** shortcut is configured in the operating system settings for switching the keyboard language, you have to left-click the **LEFT ALT** key and right-click the **SHIFT** key).

To ensure protection of data entered at the Virtual Keyboard, you should restart your computer after Kaspersky PURE is installed.

Virtual Keyboard can be opened in one of the following ways:

- from the context menu of the application icon in the taskbar notification area;
- from the main application window;
- from the window of the Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome browsers;
- using the quick launch icon of the Virtual Keyboard in entry fields on websites;

You can configure the display of the quick launch icon in entry fields on websites.

- using a combination of keys at the computer keyboard.
To open Virtual Keyboard from the context menu of the application icon in the taskbar notification area, select Tools → Virtual Keyboard from the context menu of the application icon (see figure below).

![Virtual Keyboard context menu](image)

*Figure 8. Kaspersky PURE icon context menu*

To open the Virtual Keyboard from the main application window:

1. Select the Password Manager section in the bottom part of the main application window.
2. In the bottom part of the window that opens, click the Virtual Keyboard button.

To open Virtual Keyboard from the browser window, click the Virtual Keyboard button in the toolbar of Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome.

To open Virtual Keyboard using the computer keyboard, press the CTRL + ALT + SHIFT + P keyboard shortcut.

To configure the display of the quick launch icon of the Virtual Keyboard in entry fields on websites:

1. Open the main application window.
2. In the top part of the window, click the Settings link.
3. In the Settings window that opens, in the Protection Center section select the Secure Data Input subsection.
4. In the right part of the window, in the Virtual Keyboard section select the Show quick launch icon in data entry fields check box and click the Settings button.
   
   The Virtual Keyboard window opens.
5. In the window that opens, set display rules for the quick launch icon:
   
   - On the Categories tab select the check boxes for categories of websites on which the quick launch icon should be displayed in entry fields.
   
   - If you want the quick launch icon to be displayed in entry fields on websites that are opened in Safe Run for Websites when using Safe Money, on the Categories tab select the Show Virtual Keyboard quick launch icon in Safe Money fields check box.
   
   - If you want to enable the display of the quick launch icon in entry fields on a specified website:
     a. On the Exclusions tab, in the Show quick launch icon on websites list click the Add button.
        
        The Show quick launch icon window opens.
b. In the window that opens, enter the URL of a website in the URL field and select one of the options of the display of the quick launch icon on that website (Show icon only on the specified web page or Show icon on the whole website).

6. Click the Apply button in the Settings window.

**SECURE KEYBOARD INPUT**

When working on the Internet, you frequently need to enter your personal data or your username and password. This happens, for example, during account registration on web sites, online shopping or Internet banking.

There is a risk that this personal information can be intercepted using hardware keyboard interceptors or keyloggers, which are programs that register keystrokes.

Secure keyboard input allows avoiding interception of data entered at the keyboard.

Secure keyboard input is only available for Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome browsers. When using other web browsers, data entered at the computer keyboard are not protected against interception.

Data input protection is not available in the Metro-style Microsoft Internet Explorer 10, as well as in Microsoft Internet Explorer 10, if the Enhanced Protected Mode check box is selected in the browser settings.

Secure keyboard input cannot protect your personal data if a website that requires entering such data has been hacked, because in this case information will be directed directly to intruders.

You can configure protection of data input from the computer keyboard on various websites. After protection of data input from the computer keyboard is configured, you do not have to take any additional actions when entering data.

To protect data entered at the computer keyboard, you should restart your computer after Kaspersky PURE is installed.

To configure protection of data input from the computer keyboard:

1. Open the main application window.

2. In the top part of the window, click the Settings link.

3. In the Settings window that opens, in the Protection Center section select the Secure Data Input subsection.

4. In the right part of the window, in the Secure keyboard input section select the Enable secure keyboard input check box and click the Settings button.

   The Secure Keyboard Input window opens.

5. In the window that opens, specify the protection scope for data input at the computer keyboard:
   - On the Categories tab select the check boxes for categories of websites on which data entered at the keyboard should be protected.
   - If you want data input from the keyboard to be protected on websites that are opened in Safe Run for Websites in Safe Money mode, on the Categories tab select the Enable secure keyboard input for Safe Money check box.
   - If you want data input at the keyboard to be protected in password fields on all websites, on the Categories tab select the Protect password fields on all websites check box.
   - If you want to enable protection of data input from the keyboard on a specified website:
     a. On the Exclusions tab, in the Enable secure keyboard input on websites list click the Add button.

       The Protected website window opens.
b. In the window that opens, enter the URL of a website in the URL field and select one of the protection options for data input on this website (Enable protection only on the specified web page or Enable protection on the whole website).

6. Click the Apply button in the Settings window.

**PASSWORD PROTECTION**

Kaspersky PURE stores and protects your personal data (such as passwords, user names, contact details, and financial data). Kaspersky PURE links passwords and accounts to the corresponding applications or websites. Personal data is contained in the storage in encrypted form. Access to the storage is protected with the master password. When the storage is unlocked, you can easily access your passwords and data. Kaspersky PURE offers an easy and convenient way to enter the password, user name, and other identity data when signing in to websites or applications, and to perform automatic sign-in.

You can access your personal data from any device that is connected to the Internet and has the application installed on it. If the device is not connected to the Internet, you can save your passwords and data on the device. As soon as the device connects to the Internet, Kaspersky PURE prompts you to synchronize your passwords and data with the password storage on remote servers.

You can additionally use Kaspersky PURE functions to:

- Create strong account passwords using Password Generator
- Synchronize your current passwords and identity data with all of your devices on which Kaspersky PURE is installed

**IN THIS SECTION**

Adding account data for automatic login .......................................................... 49
Using Password Generator ................................................................................. 50
Adding a new login and password pair .............................................................. 51

**ADDING ACCOUNT DATA FOR AUTOMATIC LOGIN**

The application can automatically sign you in to websites and applications by entering your login and password. The application uses accounts for automatic sign-in.

You can create accounts of two types:

- Web accounts used for signing in to websites
- Application accounts for signing in to applications, such as email clients

To add a new Internet account in the main window of Kaspersky PURE:

1. Open the main application window and click the Password Manager button.
   The Password Manager window opens.

2. Click the Passwords and data button.
   The contents of the passwords and data storage are displayed.

3. Open the Internet section in the Password Manager window.
   Fields for entering account details appear in the right part of the window.
4. Enter the account name in the **Account name** field in the upper part of the window. Click the **✓** button. The account name will be saved.

5. In the **URL** field, type the address of the website where the new account will be used to sign in.

6. Enter the login name for website login in the **Login** field.

7. In the **Password** text box, enter the password for the account. To create a password automatically, click the **Password generator** link.

8. In the bottom part of the window, click the **Add** button. The new account appears in the list of accounts in the **Internet** section.

**To add a new application account:**

1. Open the main application window and click the **Password Manager** button. The Password Manager window opens.

2. Click the **Passwords and data** button. The contents of the passwords and data storage are displayed.

3. Open the **Applications** section. Click the **Add application account** button.

4. Enter the account name in the **Account name** field in the upper part of the window. Click the **✓** button. The account name will be saved.

5. In the **Application** field, type the path to the executable file of the application into which you will be signing in with the account.

6. Enter the login name for application login in the **Login** field.

7. In the **Password** text box, enter the password for the account. To create a password automatically, click the **Password generator** link.

8. In the bottom part of the window, click the **Add** button. The created account appears in the list of accounts in the **Applications** section.

**Using Password Generator**

Data security directly depends on password strength. Data may be exposed to risk in the following cases:

- The same password is used for all accounts
- Passwords are too weak
- Easy-to-guess information is used as a password (such as names or dates of birth of family members)

To keep your data secure, Kaspersky PURE enables you to generate unique and strong account passwords using Password Generator.

A password is considered strong if it consists of four or more characters and contains special characters and numerals, upper-case and lower-case letters.
To create a strong password using Password Generator:

1. Open the main application window and click the Password Manager button.
   The Password Manager window opens.

2. Click the Password Generator button.
   You can also use Password Generator while specifying the account password. To call up Password Generator, click the Password Generator link in the account management area next to the password entry field.

3. In the Password Generator window that opens, specify the number of password characters in the Password length field.
   A password can be 4 to 99 characters long. Longer passwords are considered stronger.

4. If necessary, configure additional settings of Password Generator by selecting or clearing check boxes opposite the relevant settings in the Advanced settings section.

5. Click the Generate button.
   The Password field shows the generated password.

**ADDING A NEW LOGIN AND PASSWORD PAIR**

Users sometimes need to use several different sets of credentials to sign in to the same website or application. Examples include using several mailboxes on the same mail server or different users accessing their social networking accounts on the same computer. When this is the case, Kaspersky PURE makes it possible to create a single account linked with the relevant website or application and specify several sets of credentials for this account.

When the relevant application or website loads, Kaspersky PURE prompts the user to select the corresponding credentials to fill in the login fields.

Kaspersky PURE automatically detects a new login when it is first used and prompts the user to add it to the account for this application or website. You can manually add new credentials for an account and edit them later. You can also use the same credentials for different accounts.

To add a new login and password pair for an account:

1. Open the main application window and click the Password Manager button.
   The Password Manager window opens.

2. Click the Passwords and data button.
   The contents of the passwords and data storage are displayed.

3. Open the Internet or Applications section depending on the type of account for which you want to add credentials.

4. Choose the relevant account in the list and click the button.

5. Select the Add login command from the context menu.

6. Enter your login to the Login field and your password to the Password field.
   To add a login and password already used for other accounts, click the button in the Login field. In the Choose credentials to link field that opens, select the account containing the required login and click the Link button.
7. If you want Password Manager to automatically insert the credentials you have created on a website or in an application, select the **Automatic sign in** check box in the lower part of the account management area.

If you do not want Password Manager to automatically insert the credentials in the login fields, clear the **Automatic sign in** check box. In this case, you can use automatic sign in by selecting the credentials you created in the context menu of the application or the quick launch button.

8. In the bottom part of the window, click the **Add** button.

The number of logins added to an account appears in the list of accounts.

**DATA ENCRYPTION**

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

By default, a single preset container with standard settings is available after Kaspersky PURE installation. Using this container requires setting a password. It is possible to create containers with custom settings.

To protect data, place it in the container and encrypt it. A password will have to be entered to access the data in the container.

To create an encrypted container:

1. Open the main application window and click the **Data Encryption** button.
2. In the window that opens, click the **Create container** button (see figure below).

![Data Encryption Window](image_url)

*Figure 9. Data encryption window*
To write data to the container:

1. Open the main application window and click the Data Encryption button.
2. In the window that opens, select the container in the list and click the Open container button.

The container opens in a Microsoft Windows Explorer window.

3. Place in it the data you want to encrypt.
4. In the Data Encryption window, click the Encrypt data button.

To gain access to the data in the container, do the following:

1. Open the main application window and click the Data Encryption button.
2. In the window that opens, select the container in the list and click the Decrypt data button.
3. In the window that opens, enter the password to obtain access to the container.
4. In the Data Encryption window, click the Open container button.

**UNUSED DATA CLEANER**

The system accumulates temporary or unused files over time. These files may use up a lot of disk space, thus impairing system performance, and may also be exploited by malware.

The temporary files are created at the launch of any applications or operating systems. But some of them remain undeleted even after you close the application or operating system. Kaspersky PURE comes with Unused Data Cleaner.

Unused Data Cleaner can detect and remove the following files:

- system event logs, where the names of all active applications are recorded;
- event logs of various applications or update utilities (such as Windows 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.

Besides the deletion of unused files from the system, the wizard deletes files which may contain confidential data (passwords, user names, registration form data). However, for complete deletion of such data, we recommend using the Privacy Cleaner Wizard (see page 57).

To start Unused Data Cleaner:

1. Open the main application window.
2. In the bottom part of the window, click the Additional Tools button.
The Additional Tools window opens (see figure below).

![Additional Tools window](image)

**Figure 10. Additional Tools window**

3. In the window that opens, in the Unused Data Cleaner section, click the Run button.

The Wizard consists of a series of screens (steps) navigated using the Back and Next buttons. To close the Wizard once it has completed its task, click the Finish button. To stop the Wizard at any stage, click the Cancel button.

Let us examine the Wizard steps in detail.

**Step 1. Starting the Wizard**

The first page of the Wizard shows information about the deletion of unused information.

Click the Next button to start the wizard.

**Step 2. Searching for unused data**

The Wizard searches the computer for unused data. The scan may take some time. Once the search is complete, the Wizard will proceed automatically to the next step.

**Step 3. Selecting actions to delete unused data**

On completing the search for unused files, the Wizard shows a list of operations that can be performed with these files.

To view the actions within a group, click the + icon to the left of the group name.
To make the Wizard perform a certain action, select the check box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, clear the box next to it.

Clearing the check boxes selected by default is not recommended. This may jeopardize the safety of your computer.

Having defined the set of actions which the Wizard will perform, click the Next button.

**Step 4. Unused Data Cleaner**

The Wizard will perform the actions selected during the previous step. The deletion of unused information may take some time.

After the clearing of unused information has been completed, the Wizard will automatically proceed to the next step.

While the Wizard is running, some files (such as the Microsoft Windows log file and 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.

**Step 5. Wizard completion**

Click the Finish button to close the Wizard.

**FILE SHREDDER**

Added security of personal data is ensured by protecting deleted information against unauthorized recovery by hackers.

Kaspersky PURE contains a permanent data deletion tool that makes data recovery using standard software tools impossible.

Kaspersky PURE makes it possible to delete data without the possibility to recover it from the following data media:

- Local drives. Deletion is possible if the user has the rights required for recording and deleting information.
- Removable drives or other devices that are recognized as removable drives (such as floppy disks, flash memory cards, USB disks, or cell phones). Data can be deleted from a flash memory card if its mechanical protection from rewriting is disabled.

You can delete the data that you can access under your personal account. Before deleting data, make sure that it is not used by running applications.

*To delete data without any possibility of recovering it:*

1. Open the main application window.
2. In the bottom part of the window, click the Additional Tools button.
The **File Shredder** window opens (see figure below).

3. In the window that opens, in the **File Shredder** section, click the **Open** button.

4. In the **File Shredder** window that opens, click the **Browse** button, and in the **Select file or folder** window that opens select the file or folder you want deleted permanently.

   Deletion of system files and folders may cause operating system malfunctions. If you select system files or folders for deletion, the application will request additional confirmation of their deletion.

5. In the **Data deletion method** drop-down list, select the requisite data deletion algorithm.

   To delete data from SSD and USB devices, as well as from network drives it is recommended to apply the Quick deletion or GOST R 50739-95 method. Other deletion algorithms can harm a network or a removable device.

6. In the window that opens, confirm the data restoration by clicking **OK**. If some files are not deleted, try to delete them again by clicking the **Retry** button in the window that opens. To select another object to delete, click the **Finish** button.
**Privacy Cleaner**

User actions on a computer are logged in the operating system. The following information is saved:

- details of search queries entered by users and websites visited
- information about applications launched, files opened and saved;
- Microsoft Windows event log entries;
- other user activity information.

Information about user actions containing confidential information may become available to intruders and unauthorized persons.

Kaspersky PURE includes the Privacy Cleaner Wizard, which cleans up traces of user activity in the system.

> To start the Privacy Cleaner Wizard:

1. Open the main application window.
2. In the bottom part of the window, select the Additional Tools section.
3. In the window that opens, in the Privacy Cleaner section, click the Run button.

The Wizard consists of a series of screens (steps) navigated using the Back and Next buttons. To close the Wizard once it has completed its task, click the Finish button. To stop the Wizard at any stage, click the Cancel button.

Let us examine the Wizard steps in detail.

**Step 1. Starting the Wizard**

Make sure the Perform user activity traces diagnostics option is selected and click the Next button to start the Wizard.

**Step 2. Searching for traces of activity**

This Wizard searches for traces of malware activities in your computer. The scan may take some time. Once the search is complete, the Wizard will proceed to the next step automatically.
Step 3. Selecting Privacy Cleaner actions

When the search is complete, the Wizard displays the detected activity traces and recommends actions to clean them up (see figure below).

![Activity traces detected and recommendations on eliminating them](image)

To view the actions within a group, click the + icon to the left of the group name.

To make the Wizard perform a certain action, select the check box to the left of the corresponding action description. By default, the Wizard performs all recommended and strongly recommended actions. If you do not wish to perform a certain action, clear the box next to it.

Clearing the check boxes selected by default is not recommended. This may jeopardize the safety of your computer.

Having defined the set of actions which the Wizard will perform, click the Next button.

Step 4. Privacy Cleaner

The Wizard will perform the actions selected during the previous step. The elimination of activity traces may take some time. To clean up certain activity traces, a computer restart may be required; the Wizard will notify you about this.

Once the activity traces have been cleaned up, the Wizard will proceed to the next step automatically.
Step 5. Wizard completion

If you wish to clean up the traces of user activity automatically whenever Kaspersky PURE completes its work, use the last screen of the Wizard to select the check box **Clean activity traces every time on Kaspersky PURE 3.0 exit**. If you plan to remove activity traces manually using the Wizard, do not select this check box.

Click the **Finish** button to close the Wizard.

**BACKUP COPYING**

The primary way to prevent the loss of vital data involves creating backup copies of data on a reliable data medium. Kaspersky PURE creates backup copies of selected data on a particular drive automatically according to schedule or manually.

You can use Home Network Control (see section “Remote management of home network protection” on page 40) to start backup tasks on home network computers and monitor the progress of such tasks.

You can use the following storage types for creating backup copies:

- local drive;
- removable drive (e.g., an external hard drive);
- network drive;
- FTP server;
- Online storage.

**DATA BACKUP**

To run backup:

1. Open the main application window and click the **Backup** button.

2. In the **Backup** window that opens, click the **Create a backup task** button.

The Backup Task Creation Wizard launches.

Let us examine the Wizard steps in detail:

a. In the data type selection window, perform one of the following operations:

   - Select one of the preset data types (files from the My Documents and Desktop folders, videos, photos, music files) to perform quick configuration.

   - Choose the **Custom files** option to manually select files to be backed up.

b. If you selected the **Custom files** option at the previous step, select the files or categories of files to be backed up in the file selection window.

When you back up data in Online storage, Kaspersky PURE does not create backup copies of data of the types that are subject to restrictions by Dropbox usage rules (see section “Using Online storage” on page 61).
c. In the storage selection window, perform one of the following operations:

- Select one of the preset storages in which backup copies will be created.

  By default, Kaspersky PURE lets you create backup copies on local and removable drives and in Online storage.

Before using Online storage for backing up your data, you have to activate Online storage (see section "Using Online storage" on page 61).

- Select an existing Online storage.

- Click the Add storage button to create a new Online storage.

  To ensure data security, we recommend using the Online storage or creating backup storages on removable drives.

d. In the schedule window, configure the task launch settings.

  If you want to back up data only once, clear the Run automatically by schedule check box.

e. In the Summary window, type the name of the new task, select the Run task when the wizard is complete check box, and click the Finish button.

RESTORING DATA FROM A BACKUP COPY

To restore data from a backup copy:

1. Open the main application window and click the Backup button.

2. Select the Restore section.

3. Select the storage where the required backup copies are located and click the Restore data button.

   The Restoring data from storage window opens.

4. In the window that opens, perform the following operations:

   a. In the Backup task drop-down list, select the task that created the relevant backup copies.

   b. In the Date drop-down list, select the date and time when the relevant backup copies were created.

   c. In the Category drop-down list, select the type of files to be restored.

5. In the file list in the lower part of the window, select the files to be restored. To do so, select check boxes next to the relevant files in the list.

   Kaspersky PURE does not allow restoring data from the Online storage if such data has been deleted via the Dropbox interface.

6. Click the Restore data button.

   The Restore window opens.
7. In the **Restore** window, specify the location for saving the restored files (the original folder or a different folder).

8. Click the **Restore selected data** button.

   The files selected for recovery will be restored and saved in the specified folder.

---

**On detecting a different version of any file selected to be restored, the application prompts the user to replace the existing file with the backup copy or save both files.**

---

**USING ONLINE STORAGE**

Online storage lets you save backup copies of your data on a remote server via the Dropbox service.

To use Online storage, create an account on the website of the backup service provider Dropbox.

You can use one and the same Dropbox account to back up data from different devices with Kaspersky PURE installed to a single Online storage.

A standard Dropbox account lets you use up to 2 GB of free space on a remote drive. If necessary, you can increase the size of Online storage on the terms of the provider of backup services. See the Dropbox website for more details on the terms of use of the web service.

Before using Online storage for backing up your data, you have to activate it.

- To activate Online storage:
  1. Open the main application window and click the **Backup** button.
  2. In the **Backup** window that opens, click the **Create a backup task** button.

      The Backup Task Creation Wizard launches.
  3. In the data type selection window, select the data category or manually specify the files that you want to back up.
  4. In the storage selection window, select the Online storage and click the **Activate now** button.

      A Dropbox account login dialog opens.
  5. In the window that opens, perform one of the following operations:

      a. Complete registration if you are not a registered Dropbox user.
      b. If you are a registered Dropbox user, log into your Dropbox account.

To finish Online storage activation, confirm that Kaspersky PURE is allowed to use your Dropbox account for backing up and restoring data. Kaspersky PURE places backup copies of saved data in a separate folder that is created in the Dropbox storage folder for applications.

After Online storage activation has been completed, the storage selection window opens. It contains a selection of online storages to choose from. For the activated Online storage, the application shows the amount of used space and the amount of free space available for data storage.
**PASSWORD-PROTECTING ACCESS TO KASPERSKY PURE SETTINGS**

A single computer may be shared by several users with various levels of experience and computer literacy. Unrestricted access of different users to Kaspersky PURE and its settings may compromise the level of computer security.

To restrict access to the application, you can set the administrator password and specify which actions should require entering this password:

- configuration of the application settings;
- backup management;
- Home Network Control (password must be the same on all computers in the network);
- Parental Control management;
- exiting the application;
- application removal.

**To password-protect access to Kaspersky PURE:**

1. Open the main application window.
2. In the top right corner of the window, click the **Settings** link.
   The application settings window opens.
3. Select the **Password** tab in the upper part of the settings window (see figure below).

![Settings window, Password section](image)

**Figure 13. Settings window, Password section**
4. In the right part of the window, select the **Enable password protection** check box and fill in the **New password** and **Confirm password** fields.

5. To change a previously created password, type it in the **Old password** field.

6. Under the **Apply password to** group of settings, specify the operations with the applications the access to which has to be password protected.

7. Click the **Apply** button to save changes.

---

A forgotten password cannot be recovered. If you have forgotten your password, contact Technical Support to restore access to Kaspersky PURE settings.

---

**Using Parental Control**

**Parental Control** allows the monitoring of actions users take on the computer and online. You can use Parental Control to restrict access to Internet resources and applications, as well as view reports on users’ activities.

Nowadays, an ever-increasing number of children and teenagers are obtaining access to computers and web resources. The use of computers and the Internet imposes a whole range of risks on children:

- loss of time and / or money when visiting chat rooms, gaming resources, online stores, auctions;
- access to websites targeted at an adult audience, such as those displaying pornography, extremism, firearms, drug abuse, and explicit violence;
- downloading of files infected with malware;
- health damage inflicted by excessive use of computer;
- contacts with unfamiliar people who may pretend to be peers to obtain personal information from under-age users, such as real name, physical address, time of day when nobody is home.

Parental Control allows you to reduce risks posed by the computer and the Internet. To do this, the following module functions are used:

- limiting the time for computer and Internet use;
- creating lists of allowed and blocked applications, as well as temporarily limiting the number of startups for allowed applications;
- creating lists of allowed and blocked websites and selection of categories of websites with content not recommended for viewing;
- enabling a safe search mode through search engines (links to websites with dubious content are not displayed in the search results);
- restricting file downloads from the Internet;
- creating lists of contacts which are allowed or blocked for communication via IM clients and social networks;
- viewing message logs from IM clients and social networks;
- blocking sending of certain personal data;
- searching for specified key words in message logs.
All these restrictions can be enabled independently from each other, which allows you to flexibly configure Parental Control for various users. For each account, you can view reports of events in the categories to be controlled that the component has logged over a specified period.

**IN THIS SECTION:**

- Configuring Parental Control .................................................................................................................. 64
- Viewing the report on a user’s activity ......................................................................................................... 64

**CONFIGURING PARENTAL CONTROL**

If you have not protected access to Kaspersky PURE settings with a password (see page 62), at the first launch of Parental Control Kaspersky PURE will suggest that you set a password to prevent unauthorized changes to the control settings. You can then configure restrictions for computer and Internet usage by all accounts on the computer.

To configure Parental Control for an account:

1. Open the main application window and click the **Parental Control** button.

   The **Computer Users** window opens, listing all user accounts created on the computer.

2. Click the **Select control level** button for the relevant account.

3. In the **Parental Control** window that opens, perform one of the following:
   - select one of the preset control levels (**Data collection**, **Child profile** or **Teenager profile**)
   - set restrictions manually:
     a. Select the **Custom restrictions** item.
     b. Click the **Settings** button.

        The **Parental Control** window opens.

     c. In the window that opens, on the **Settings** tab, select the type of restriction in the left part of the window and specify the control settings in the right part of the window.

     d. Click the **OK** button to save the configured control settings.

4. Click the **OK** button in the **Parental Control** window.

**VIEWING THE REPORT ON A USER’S ACTIVITY**

You can access reports on the activity of each user account under Parental Control, reviewing individually each category of controlled events.

To view a report on the activity of a controlled user account:

1. Open the main application window.

2. In the lower part of the window, select the **Parental Control** section.

3. In the section containing the account in the window that opens, click the **`gear`** button.

   The **Parental Control** window opens.
4. Select the **Reports** tab.

5. Use the left part of the window that opens to select the category of supervised operations or content, for example, **Internet Usage** or **Private Data**.

   A report of actions and content being supervised will be displayed in the right part of the window.

### PAUSING AND RESUMING COMPUTER PROTECTION

Pausing protection means temporarily disabling all protection components for some time.

*To pause protection of your computer:*

1. In the context menu of the application icon in the taskbar notification area, select the **Pause protection** item.

   The **Pause protection** window opens (see figure below).

   ![Pause protection window](image)

   *Figure 14. Pause protection window*

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

   - **Pause for the specified time** – protection will be enabled on expiration of the time interval selected from the drop-down list below.
   - **Pause until reboot** – protection will be enabled after the application is restarted or the operating system is rebooted (provided that automatic application launch is enabled).
   - **Pause** – protection will be resumed when you decide to resume it.

*To resume computer protection,*

select the **Resume protection** item in the context menu of the application icon in the taskbar notification area.
VIEWING COMPUTER PROTECTION REPORT

Kaspersky PURE maintains operation reports for each of the protection components. The report offers statistical information on the operation of the application (for example, the number of malicious objects detected and neutralized during a particular period, the number of application updates during the same period, the number of spam messages detected, and much more).

To view the report on computer protection:

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

   The Computer Protection window opens.

2. Click the Reports link in the upper part of the window to open the computer protection reports window.

   Computer protection reports are shown as graphs in the Reports window.

3. If you want to view a detailed application activity report (for example, a report on the activity of each component), click the Detailed report button in the lower part of the Report window.

   The Detailed report window opens, displaying data in the form of a table. For a convenient view of reports, you can select various sorting options.

RESTORING THE DEFAULT APPLICATION SETTINGS

You can restore the default application settings recommended by Kaspersky Lab for Kaspersky PURE, at any time. The settings can be restored using the Application Configuration Wizard.

Application Configuration Wizard sets the Recommended security level for all protection components. When restoring the recommended security level, you can save the previously specified values for some of the settings of application components.

To restore the recommended application settings:

1. Open the main application window.

2. In the top part of the window, click the Settings link.

3. In the Settings window that opens, run Application Configuration Wizard in one of the following ways:

   - click the Restore link in the bottom left corner of the window;
• in the upper part of the window, select the Advanced Settings section, Manage Settings subsection and click the Restore button in the Restore default settings section (see figure below).

![Settings window, Manage Settings subsection](image)

Figure 15. Settings window, Manage Settings subsection

Let us examine the Wizard steps in detail.

**Step 1. Starting the Wizard**

Click the Next button to proceed with the Wizard.
Step 2. Restore settings

This Wizard window shows which Kaspersky PURE protection components have settings that differ from the default value because they were either changed by the user or accumulated by Kaspersky Internet Security through training (Firewall or Anti-Spam). If special settings have been created for any of the components, they will also be shown in the window (see figure below).

![Figure 16. Restore settings window](image)

Examples of special settings would be: white and black lists of phrases and addresses used by Anti-Spam, lists of trusted URLs and trusted ISP telephone numbers, exclusion rules created for application components, and Firewall packet and application filtering rules.

The special settings are created when working with Kaspersky PURE with regard for individual tasks and security requirements. Kaspersky Lab recommends that you save your special settings when restoring the default application settings.

Select check boxes opposite the settings to be retained and click Next.

Step 3. System analysis

At this stage, information is collected about the applications that are included with Microsoft Windows. These applications are added to the list of trusted applications that are free from restrictions on the actions they perform in the system.

Once the analysis is complete, the Wizard will proceed automatically to the next step.

Step 4. Completing restoration

To complete the Wizard, click the Finish button.
IMPORTING THE APPLICATION SETTINGS TO KASPERSKY PURE INSTALLED ON ANOTHER COMPUTER

Once you have configured the product, you can apply its settings to Kaspersky PURE installed on another computer. Consequently, the application will be configured identically on both computers. This is a helpful feature when, for example, Kaspersky PURE is installed on your home computer and in your office.

The settings of Kaspersky PURE can be transferred to another computer in three steps:

1. Exporting the application settings to a configuration file.
2. Transferring a configuration file to another computer (for example, by email or on a removable medium).
3. Applying the settings from a configuration file to the application installed on another computer.

To save Kaspersky PURE settings in a configuration file:

1. Open the main application window.
2. In the top part of the window, click the Settings link.
3. In the upper part of the Settings window, in the Additional section select the Manage Settings subsection.
4. Click the Export button in the Manage Settings subsection.
5. In the window that opens, enter the name of the configuration file and specify the location to which it should be saved.
6. Click OK.

To apply the settings from the configuration file to the application installed on another computer:

1. Open the main application window.
2. In the top part of the window, click the Settings link.
3. In the upper part of the Settings window, in the Additional section select the Manage Settings subsection.
4. Click the Import button in the Manage Settings subsection.
5. In the window that opens, select the file from which you wish to import the Kaspersky PURE settings.
6. Click OK.

CREATING AND USING A RESCUE DISK

The rescue disk is a copy of Kaspersky Rescue Disk stored on a removable drive (CD or USB device).

You can use Kaspersky Rescue Disk for scanning and disinfecting infected computers that cannot be disinfected using other methods (e.g., with anti-virus applications).

IN THIS SECTION:

Creating a Rescue Disk ........................................................................................................................................... 70
Booting the computer using the Rescue Disk............................................................................................................. 72
Creating a Rescue Disk

Creating a Rescue Disk consists in creating a disk image (ISO file) with the up-to-date version of Kaspersky Rescue Disk, and writing it on a removable medium.

The original disk image can be downloaded from a Kaspersky Lab server or copied from a local source.

The Rescue Disk is created using the Kaspersky Rescue Disk Creation Wizard. The rescuecd.iso file created by the Wizard is saved on your computer's hard drive:

- in Microsoft Windows XP – in the following folder: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP13\Data\Rdisk;
- in Microsoft Windows Vista, Microsoft Windows 7, and Microsoft Windows 8 operating systems – in the following folder: ProgramData\Kaspersky Lab\AVP13\Data\Rdisk.

To create a rescue disk:

1. Open the main application window.
2. In the bottom part of the window, select the Additional Tools section.
3. In the Kaspersky Rescue Disk window that opens, click the Save button. The Rescue Disk Creation Wizard window opens.

The Wizard consists of a series of screens (steps) navigated using the Back and Next buttons. To close the Wizard once it has completed its task, click the Finish button. To stop the Wizard at any stage, click the Cancel button.

Let us examine the Wizard steps in detail.

Step 1. Starting the Wizard. Finding an existing disk image

The first page of the Wizard shows information about the Kaspersky Rescue Disk application.

If the Wizard has detected a previously created disk image in the folder made for this purpose (see above), the Use existing Kaspersky Rescue Disk image check box will be shown on the first page of the Wizard. Select the check box to use the detected file as the original ISO image and go directly to the Updating disk image step (see below). If you do not want to use the located disk image, clear this check box. The Wizard will proceed to the Select disk image source page.

Step 2. Select disk image source

If you have selected the Use existing Kaspersky Rescue Disk image check box on the first wizard page, then this step will be skipped.

At this step, you should select the disk image source from the list of options:

- If you already have a recorded Kaspersky Rescue Disk or its image (an ISO file) saved on your computer or another local network resource, select the option Copy ISO image from local or network drive.

- If you do not have a recorded Rescue Disk image and you want to download it from a Kaspersky Lab server (the file size is approximately 175 MB), select the option Download ISO image from Kaspersky Lab server.
Step 3. Copying (downloading) disk image

If you have selected the **Use existing Kaspersky Rescue Disk image** check box on the first wizard page, then this step will be skipped.

If you have selected the option to **Copy ISO image from local or network drive** during the previous step, click the **Browse** button. After you have specified the path to the file, click the **Next** button. The disk image copying progress is displayed in the Wizard window.

If you have selected **Download ISO image from Kaspersky Lab server** during the previous step, disk image downloading progress is displayed immediately.

When copying or downloading the ISO image is complete, the Wizard automatically proceeds to the next step.

Step 4. Updating ISO image file

The updating procedure for the ISO image file comprises the following operations:

- updating application databases
- update of configuration files.

Configuration files determine whether the computer can be booted from a removable medium (such as a CD / DVD or a USB flash drive with Kaspersky Rescue Disk) created by the Wizard.

When updating the application databases, those distributed at the last update of Kaspersky PURE are used. If databases are out of date, it is recommended that you run the update task and launch the Kaspersky Rescue Disk Creation Wizard again.

To begin updating the disk image file, click the **Next** button. The updating progress will be displayed in the Wizard window.

Step 5. Recording the disk image on the drive

At this step, the Wizard announces that the disk image has been created successfully and offers to write the disk image to a drive.

Specify the drive to which Kaspersky Rescue Disk should be written:

- To record the disk image on a CD / DVD, select **Record to CD / DVD** and specify a medium, on which you want to record the disk image.

- To write to a USB device, select the option **Record to USB drive** and specify the device to which you want to write the disk image.

- To save the disk image on the hard drive of your computer or another computer that you can access over the network, select the option **Save the disk image to file on local or network drive** and specify the folder to which you want to save the disk image and specify the name of the ISO file.

Kaspersky Lab specialists do not recommend saving the disk image on devices that are not intended exclusively for data storage, such as smartphones, mobile phones, pocket PCs, or MP3 players. After being used to store the disk image, such devices may malfunction.

Step 6. Wizard completion

To complete the Wizard, click the **Finish** button. You can use the newly created Rescue Disk to boot the computer (see page 72) if you cannot boot it and run Kaspersky Internet Security in normal mode due to an impact caused by viruses or malware.
**BOOTING THE COMPUTER USING THE RESCUE DISK**

If the operating system cannot be started as a result of a virus attack, use the Rescue Disk.

To boot the operating system, you should use a CD / DVD or a USB flash drive with Kaspersky Rescue Disk copied on it (see section "Creating a Rescue Disk" on page 70).

Loading a computer from a removable drive is not always possible. In particular, this mode is not supported by some obsolete computer models. Before shutting down your computer for further booting from a removable data medium, make sure that this operation can be performed.

To boot your computer from the Rescue Disk:

1. In the BIOS settings, enable booting from a CD / DVD or a USB device (for detailed information, please refer to the documentation for your computer’s motherboard).

2. Insert a CD / DVD into the CD / DVD drive of an infected computer or connect a USB flash device with Kaspersky Rescue Disk copied on it.

3. Restart your computer.

For detailed information about the use of the Rescue Disk, please refer to the Kaspersky Rescue Disk User Guide.
CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

**IN THIS SECTION**

- How to obtain technical support .............................................................. 73
- Technical support by phone .......................................................................................... 73
- Obtaining technical support via My Kaspersky Account ........................................... 74
- Creating a system state and AVZ script usage report .................................................. 75

**HOW TO OBTAIN TECHNICAL SUPPORT**

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application (see section “Sources of information about the application” on page 9), we recommend that you contact Kaspersky Lab’s Technical Support Service. Technical Support specialists will answer your questions about installing and using the application.

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

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

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.

- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact Technical Support specialists through a request form.

Technical support is only available to users who acquired the commercial license. No technical support is provided to users of trial versions.

**TECHNICAL SUPPORT BY PHONE**

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

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/details). This will allow our specialists to help you more quickly.
OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

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

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

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

- Contact Technical Support and the Virus Lab.
- Contact Technical Support without using email.
- Track the status of your requests in real time.
- View a detailed history of your Technical Support requests.
- Receive a copy of the key file if it is lost or deleted.

Technical Support by email

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

In the fields of the online request form, specify the following data:

- Request type
- Application name and version number
- Request description
- Customer ID and password
- email address

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

Online request to the Virus Lab

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

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

- Unknown malware – You suspect that a file contains a virus, but Kaspersky PURE does not identify it as infected.
  
  Virus Lab specialists analyze malicious code that is sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- False positive – Kaspersky PURE classifies the file as a virus, but you are sure that the file is not a virus.

- Request for description of malicious program – You want to receive the description of a virus that Kaspersky PURE detects, based on the name of the virus.
You can also send requests to the Virus Lab from the page with the request form (http://support.kaspersky.com/virlab/helpdesk.html) without being registered in My Kaspersky Account. On this page, you do not have to specify the application activation code.

**Creating a system state and AVZ script usage report**

After you notify Technical Support Service specialists of a problem encountered, they may ask you to create a report that should contain information about your operating system, and send it to the Technical Support Service. Technical Support Service specialists may also ask you to create a file with technical information on system performance. This file helps to track down step-by-step execution of application commands and detect the stage of application operation at which the error occurs.

After Technical Support Service specialists analyze the data that you have sent, they can create an AVZ script and send it to you. Running AVZ scripts allows you to analyze active processes for malicious code, scan the system for malicious code, disinfect / delete infected files, and create reports on results of system scans.

---

**In this section:**

- Creating a system state report .......................................................... 75
- Collecting technical data on application performance ................................ 76
- Sending data files .............................................................................. 76
- AVZ script execution ........................................................................ 77

---

**Creating a system state report**

**To create a system state report:**

1. Open the main application window.
2. Click the **Support** link in the lower part of the main window to open the **Support** window.
   
   Click the **Support Tools** button.
3. In the **Support Tools** 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 the sysinfo.zip archive. Once the information gathering process is complete, you can view the report.

**To view a report:**

1. Open the main application window.
2. Click the **Support** link in the lower part of the main window to open the **Support** window.
   
   Click the **Support Tools** button.
3. In the **Support Tools** window that opens, click the **View report** button.
4. Open the sysinfo.zip archive which contains the report files.
COLLECTING TECHNICAL DATA ON APPLICATION PERFORMANCE

You can use event logging to collect technical information on the performance of the application and the operating system. A report on logged events enables Technical Support Service specialists to analyze the problem that occurred during application operation.

To collect and save information about a problem in application operation:

1. Open the main application window.
2. Click the Support link in the lower part of the main window to open the Support window.
3. In the Support window, click the Support Tools button.
4. In the Support Tools section, select the importance level of events in the Trace level drop-down list.
   You can select the following levels of importance of events recorded in the report:
   • Important. Kaspersky PURE fills the report with information about events that are potentially important for the computer’s security, such as detection of a probably infected object or a suspicious activity in the system.
   • Recommended. Kaspersky PURE fills the report with information about important events, as well as events that are not of primary importance in the computer security.
   • All. Kaspersky PURE generates a detailed report on all events that can be used for the application diagnostics.
5. To start the event logging process, click the Enable traces button.
6. Click the Support window and reproduce the situation in which the application encounters the problem.
7. After reproducing the situation, return to the Support Tools section and click the Disable traces button in the Support window.
   Kaspersky PURE stops logging technical information about the performance of the application and the entire operating system.

After collecting technical operation on the performance of the application, you can send the collected data to the Kaspersky Lab Technical Support Service.

SENDING DATA FILES

After collecting technical data on application performance and creating the system status report, you need to send them to Kaspersky Lab Technical Support experts.

You will need a request number to upload data files to the Technical Support server. This number is available in My Kaspersky Account on the Technical Support website while your request is active.

To upload the data files to the Technical Support server:

1. Open the main application window.
2. Click the Support link in the bottom part of the window to open the Support window.
3. In the window that opens, click the Support Tools button.
   The Support Tools window opens.
4. In the window that opens, click the Send service data to Technical Support button.
   The Send report window opens.
5. Select the check boxes next to the data that you want to send to the Technical Support Service and click the Send button.
   The Enter request number window opens.
6. Specify the number assigned to your request by contacting Technical Support through My Kaspersky Account and click the OK button.

The selected data files are packed and sent to the Technical Support Service server.

If you cannot connect to Technical Support for some reason, the data files can be stored on your computer and later sent from My Kaspersky Account.

To save data files on a disk:

1. Open the main application window.
2. Click the Support link in the bottom part of the window to open the Support window.
3. In the window that opens, click the Support Tools button.
4. The Support Tools window opens.
5. In the window that opens, click the Send service data to Technical Support button.
   The Send report window opens.
6. Select the check boxes next to the data that you want to send to the Technical Support Service and click the Send button.
   The Enter request number window opens.
7. Click the Cancel button and confirm saving the files on the disk by clicking the Yes button in the window that opens.
   The archive saving window will open.
8. Specify the archive name and confirm saving.

The created archive can be sent to Technical Support from My Kaspersky Account.

AVZ script execution

You are advised not to change the text of an AVZ script received from Kaspersky Lab experts. If problems occur during script execution, contact the Technical Support Service (see section “How to obtain technical support” on page 73).

To run the AVZ script:

1. Open the main application window.
2. Click the Support link in the bottom part of the window to open the Support window.
3. In the window that opens, click the Support Tools button.
   The Support Tools window opens.
4. In the window that opens, click the Run script button.
   The AVZ script execution window opens.
5. Copy the text from the script sent by Technical Support Service specialists, paste it to the entry field in the window that opens, and click the Next button.
   The script is running then.

If the script is successfully executed, the Wizard closes automatically. If an error occurs during script execution, the wizard shows a corresponding message.
GLOSSARY

A
ACTIVATING THE APPLICATION
Switching the application into full-function mode. Application activation is performed by the user during or after the application installation. The user should have an activation code to activate the application.

APPLICATION MODULES
Files included in the Kaspersky Lab installation package that are responsible for performing its main tasks. A particular executable module corresponds to each type of 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.

AVAILABLE UPDATE
A package of updates for the modules of a Kaspersky Lab application including a set of urgent patches released during a certain time interval, and modifications to the application architecture.

B
BACKUP FOLDER
Disk space or removable drive selected for creating backup copies of files during backup tasks.

BLOCKING AN OBJECT
Denying access to an object from external applications. A blocked object cannot be read, executed, changed, or deleted.

C
COMPRESSED FILE
An archive file that contains a decompression program and instructions for the operating system for executing it.

CONTAINER
An encrypted object designed for storing confidential data. A container is a password-protected removable virtual drive storing files and folders.

The Kaspersky PURE application has to be installed on the computer for the container functionality to be available.

D
DATABASE UPDATE
A function performed by a Kaspersky Lab application that enables it to keep computer protection up-to-date. During the update, an application downloads updates for its databases and modules from Kaspersky Lab’s update servers and automatically installs and applies them.

DATABASE OF MALICIOUS WEB ADDRESSES
A list of web addresses whose content may be considered to be dangerous. The list was created by Kaspersky Lab specialists. It is regularly updated and is included in the Kaspersky Lab application package.

DATABASE OF PHISHING WEB ADDRESSES
List of web addresses which are defined as phishing by Kaspersky Lab specialists. The database is regularly updated and is part of the Kaspersky Lab application.
**Databases**
Databases that contain information about computer security threats that are known to Kaspersky Lab at the time of release of the databases. Records that are contained in databases allow detecting malicious code in scanned objects. The databases are created by Kaspersky Lab specialists and updated hourly.

**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 whatever reason, cannot be disinfected.

**Digital signature**
An encrypted block of data embedded in a document or application. A digital signature is used to identify the document or application author. To create a digital signature, the document or application author must have a digital certificate proving the author’s identity.

A digital signature lets you verify the data source and data integrity and protect yourself against counterfeits.

**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.

**Disinfection**
A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

**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 disk’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 scanning of boot sectors for viruses and disinfecting them if an infection is found.

**Domain name service (DNS)**
A distributed system for converting the name of a host (a computer or other network device) to an IP address. DNS functions in TCP/IP networks. As a special case, DNS can also store and process reverse requests and determine 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.

**Event severity**
Property of an event encountered during the operation of a Kaspersky Lab application. There are four severity levels:

- Critical event.
- Error.
- Warning.
- Info.

Events of the same type can have different severity levels depending on the situation in which the event occurred.
F

FALSE POSITIVE
A situation when a Kaspersky Lab application considers a non-infected object to be infected because its code is similar to that of a virus.

FILE MASK
Representation of a file name using wildcards. The standard wildcards used in file masks are * and ?, where * represents any number of any characters and ? stands for any single character.

H

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 recipient and the date.

HEURISTIC ANALYZER
A technology for detecting threats information about which has not yet been added to Kaspersky Lab databases. The heuristic analyzer allows detecting objects behaving in a way that can pose a security threat to the system. Objects detected by the heuristic analyzer are considered probably infected. For example, an object may be considered probably infected if it contains sequences of commands that are typical of malicious objects (open file, write to file).

I

ICHECKER TECHNOLOGY
A technology that allows increasing the speed of anti-virus scanning by excluding objects that have remained unchanged since their last scan, provided that the scan parameters (the databases and the settings) have not been altered. 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 file that was scanned by a Kaspersky Lab application and assigned 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 have changed the archive content by adding a new object to it, modified the scan settings, or updated the application databases, the archive will be re-scanned.

Limitations of iChecker technology:

- this technology does not work with large 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.

INCOMPATIBLE APPLICATION
An anti-virus application from a third-party developer or a Kaspersky Lab application that does not support management through Kaspersky PURE.

INFECTED OBJECT
An object a segment of whose code completely matches a section of a known threat. Kaspersky Lab does not recommend using such objects.
**Internet Protocol (IP)**

The basic protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations for transmitting data from one computer to another and serves as the foundation for higher-level protocols like TCP and UDP. It manages 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 makes it possible to meet the demands of the constantly growing Internet using the relatively restricted IPv4 address space.

**Kaspersky Lab update servers**

Kaspersky Lab HTTP servers to which the updated anti-virus database and the application modules are uploaded.

**Kaspersky Security Network (KSN)**

An infrastructure of online services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Lab applications to unknown threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

**Keylogger**

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.

**License term**

The time period during which you have access to the application features and rights to use additional services.

**Master password**

A single password that protects the Password Manager database and provides access to data.

**Message deletion**

The method of processing an email message where the message is physically removed. We recommend that this method be applied to messages that definitely contain spam or malware. Before deleting a message, a copy of it is saved in Quarantine (unless this option is disabled).

**Obscene message**

Email message containing offensive language.

**Online vault**

Method of data storage on remote, often geographically distributed servers. Online storage simplifies data synchronization across different computers and mobile devices. An Internet connection is required to use Online storage.

**Phishing**

A kind of Internet fraud which consists in sending email messages with the purpose of stealing confidential information, most often in the form of financial data.
**Probable spam**
A message that cannot be unambiguously considered spam, but has several spam attributes (e.g., certain types of mailings and advertising messages).

**Probably infected object**
An object whose code contains a modified segment of code of a known malware, or an object resembling this malware in the way it behaves.

**Program settings**
Application settings which are common for all task types, regulating the application’s operation as a whole, such as application performance settings, report settings, and Quarantine settings.

**Protected browser**
Browser launched in Safe Money mode. Safe Run for Websites is launched when you visit an online banking website, protecting user data against theft. In this case, the standard browser used for accessing the website displays a message informing you of the protected browser startup.

**Protection Center**
An application module providing comprehensive protection of the computer against various threats. Protection Center provides computer protection against viruses, spam, and network attacks. The module comprises the Update, System Watcher, and Quarantine components.

**Protection status**
Current protection status, which defines the level of computer security.

**Protocol**
A 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, FTP, and NNTP.

**Proxy server**
A 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 (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 for certain purposes.

**Q**

**Quarantine**
A dedicated storage to which the application places backup copies of files that have been modified or deleted during disinfection. Copies of files are stored in a special format, imposing no threat for the computer.

**R**

**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, while infected or probably infected objects are processed according to the task settings (disinfected or removed).

**Restoration**
Relocation of the original object from Quarantine or Backup to its original folder where the object had been stored before it was quarantined, disinfected or deleted, or to a user-defined folder.
**Rootkit**
A program or a set of programs for hiding traces of an intruder or malware in the operating system.

On Windows-based operating systems, a rootkit usually means a program that penetrates into the operating system and intercepts system functions (Windows APIs). Above all, interception and modification of low-level API functions allow such a program to make its presence in the operating system quite stealthy. A rootkit can usually also mask the presence of any processes, folders, and files that are stored on a disk drive, in addition to registry keys, if they are described in the configuration of the rootkit. Many rootkits install their own drivers and services on the operating system (these also are "invisible").

**Safe Money**
An application module that protects confidential data entered by the user on banking and e-money websites and prevents theft of money during online payments.

**Script**
A small computer program or an independent part of a program (function) which, as a rule, has been developed to execute a specific task. It is most often used with programs that are embedded in hypertext. Scripts are run, for example, when you open specified websites.

If real-time protection is enabled, the application tracks the launching of scripts, intercepts them, and scans them for viruses. Depending on the results of scanning, you may block or allow the execution of a script.

**Security level**
The security level is defined as a predefined collection of settings for an application component.

**Spam**
Unsolicited mass email mailings, most often including advertising messages.

**Startup objects**
A set of applications needed for the launch and correct operation of the operating system and software on the computer. These objects are executed every time the operating system is started. There are viruses capable of infecting startup objects in particular, which may prevent the operating system from loading.

**Subnet mask**
The subnet mask (also known as netmask) and network address determine the addresses of computers on a network.

**Task**
Functions performed by Kaspersky Lab’s application are implemented as tasks, such as: Real-time file protection, Full computer scan, Database update.

**Task settings**
Application operating settings which are specific for each task type.

**Threat level**
An index showing the probability of an application posing a threat to the operating system. The threat level is calculated using heuristic analysis based on two types of criteria:

- static (such as information about the executable file of an application: size, creation date, etc.);
- dynamic, which are used while simulating the application’s operation in a virtual environment (analysis of the application’s requests to system functions).
Threat level allows detecting behavior typical of malware. The lower the threat level is, the more actions the application will be allowed to perform in the system.

**Traffic scan**
Real-time scanning that uses information from the current (latest) version of the databases for objects transferred over all protocols (for example, HTTP, FTP, etc.).

**Unknown virus**
A new virus that is not yet registered in the databases. The application usually detects unknown viruses in objects by means of the heuristic analyzer. Such objects are labeled as probably infected.

**Update**
The procedure of replacing/adding new files (databases or application modules) retrieved from the Kaspersky Lab update servers.

**Update package**
A file package for updating application modules. A Kaspersky Lab's application copies update packages from Kaspersky Lab's update servers and automatically installs and applies them.

**Urgent updates**
Critical updates to Kaspersky Lab application modules.

**Virus outbreak**
A series of deliberate attempts to infect a computer with a virus.
KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world’s top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey “TGI-Russia 2009”.

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company’s activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab’s products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab’s centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab’s products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab’s virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. Kaspersky Lab’s Anti-Virus database is updated hourly; and the Anti-Spam database every five minutes.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company’s innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab’s main achievement is the loyalty of its users worldwide. The company’s products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab official site: http://www.kaspersky.com
Virus encyclopedia: http://www.securelist.com
Anti-virus laboratory: newvirus@kaspersky.com (only for sending probably infected files in archive format)
http://support.kaspersky.com/virlab/helpdesk.html (for queries addressed to virus analysts)
Kaspersky Lab web forum: http://forum.kaspersky.com
INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Google Chrome is a trademark owned by Google, Inc.

Intel, Pentium and Atom are trademarks of Intel Corporation registered in the United States of America and elsewhere.

Microsoft, Windows, Windows Vista and Internet Explorer are trademarks of Microsoft Corporation registered in the United States of America and elsewhere.

Mozilla and Firefox are trademarks of Mozilla Foundation.
INDEX

A
Account ........................................................................................................................................... 49
Activation code .................................................................................................................................. 26
Anti-Spam
hints ................................................................................................................................................ 38
Application activation
activation code ............................................................................................................................. 26
license ............................................................................................................................................... 24

B
Backup copying .................................................................................................................................. 59

C
Computers
managed ........................................................................................................................................... 40

D
Data
Encryption ........................................................................................................................................ 52
Databases
manual update .................................................................................................................................. 31
Default settings ............................................................................................................................... 66

E
Encryption
data encryption .................................................................................................................... 52
End User License Agreement .......................................................................................................... 24
Event log ........................................................................................................................................... 66

H
Hardware requirements ...................................................................................................................... 15

I
Importing / exporting the settings ................................................................................................... 69
Installing the application .................................................................................................................. 16

K
Kaspersky Lab .................................................................................................................................. 85
Key .................................................................................................................................................... 24

L
License .............................................................................................................................................. 24
activation code .................................................................................................................................... 24
End User License Agreement ........................................................................................................... 24

N
Network protection status .................................................................................................................. 40

P
Parental Control
<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>component operation</td>
<td>64</td>
</tr>
<tr>
<td>Password manager account</td>
<td>49</td>
</tr>
<tr>
<td>Post-infection Microsoft Windows troubleshooting</td>
<td>36</td>
</tr>
<tr>
<td>Protection status</td>
<td>30</td>
</tr>
</tbody>
</table>

### Q
- Quarantine
  - restoring an object | 34 |

### R
- Remote administration of the application | 40 |
- Reports | 66 |
- Rescue Disk | 69 |
- Restoring the default settings | 66 |
- Restricting access to the application password protection | 62 |
- Run task
  - scanning | 32 |
  - update | 31 |
  - Vulnerability Scan | 34 |

### S
- Scan
  - starting the task | 32 |
  - vulnerability scan | 34 |
- Software requirements | 15 |
- Statistics | 66 |
- Storages
  - Backup | 59 |
  - Quarantine | 34 |

### T
- Tasks
  - backup | 59 |

### U
- Update | 31 |

### V
- Virtual Keyboard | 46 |