# **Kaspersky Rescue Disk**

# **USER GUIDE**

APPLICATION VERSION: 10.0



#### Dear User!

Thank you for choosing our product. We hope that this documentation helps you in your work and provides answers to the most questions you may have.

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

This document and the graphic images it contains may be used exclusively for information, non-commercial or personal purposes.

This document is subject to change without prior notice. For the latest version of this document please refer to Kaspersky Lab's website at <a href="http://www.kaspersky.com/docs">http://www.kaspersky.com/docs</a>.

Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document for which the rights are held by third parties, or for the potential damages associated with using such documents.

This document involves the registered trademarks and service marks which are the property of their respective owners.

Revision date: 30.04.2010

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

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

#### END USER LICENSE AGREEMENT

Kaspersky Lab ZAO (the "Rightholder") is an owner of all rights, whether exclusive or otherwise to the Software.

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

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

The Rightholder hereby grants You a non-exclusive perpetual license to store, load, install, execute, and display (to "use") the free of charge Software that will substantially perform within the scope of functionality set forth on <a href="http://support.kaspersky.com/viruses">http://support.kaspersky.com/viruses</a>.

Technical support is available only to users of Kaspersky Anti-Virus 2011 and Kaspersky Internet Security 2011 products.

Technical support service: <a href="http://support.kaspersky.com">http://support.kaspersky.com</a>

You shall not emulate, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation.

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

THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DICLOSED TO THE RIGHTHOLDER.

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

# **TABLE OF CONTENTS**

ABOUT THIS HELP	6
In this document	6
Legend	8
ADDITIONAL SOURCES OF INFORMATION	9
Sources of information to research on your own	9
Discussing Kaspersky Lab applications on the web forum	10
Contacting the User documentation development group	10
KASPERSKY RESCUE DISK	11
What's new	12
Hardware and software requirements	13
WRITING KASPERSKY RESCUE DISK TO A REMOVABLE DRIVE	14
Preparing to write	14
Writing Kaspersky Rescue Disk	14
LOADING KASPERSKY RESCUE DISK	16
Preparing to load	16
Kaspersky Rescue Disk loading procedure	16
WORKING WITH KASPERSKY RESCUE DISK IN GRAPHIC MODE	18
Kaspersky Rescue Disk interface	
Taskbar	
Anti-Virus interface	20
Additional tools	23
Starting and stopping Anti-Virus	24
Starting Anti-Virus	25
Stopping Anti-Virus	25
Computer protection status	25
Objects scan	27
About scanning objects for viruses	27
Starting and stopping the objects scan	28
Creating a list of objects to scan	29
Update	30
About the update	
Starting and stopping the update	
Rolling back the last update	
Quarantine and Backup	
About Quarantine	
Actions with quarantined objects	
About Backup	
Reports	
About reports	
Selecting task to create a report	
Managing information grouping in the report	
Displaying data on the screen	
Saving report to a file	

Using complex filtering	41
Events search	42
Extended statistics display	43
Advanced application settings	44
Objects scan	44
Update	51
Threats and exclusions. Trusted zone	53
Notifications	57
Reports and storages	60
Closing Kaspersky Rescue Disk	62
WORKING WITH KASPERSKY RESCUE DISK IN TEXT MODE	63
About text mode	63
Working with file manager	64
Network setup	64
Starting the Kaspersky Rescue Disk console	64
Virus scan	65
Kaspersky Rescue Disk update	65
Rolling back to the previous databases	65
Viewing Help	
Closing Kaspersky Rescue Disk	65
Working with command prompt	66
Command prompt syntax	
Virus scan	
Kaspersky Rescue Disk update	
Rolling back the last update	
Viewing Help	
Closing Kaspersky Rescue Disk	69
HARDWARE INFORMATION	70
RESTRICTIONS IN THE APPLICATION OPERATION	71
CONTACTING THE TECHNICAL SUPPORT SERVICE	72
My Kaspersky Account	72
Technical support by phone	73
Creating and saving the trace file	73
GLOSSARY	74
KASPERSKY LAB ZAO	77
INFORMATION ON THIRD-PARTY CODE	78
Program code	78
Developer tools	78
Distributable program code	78
Other information	78
INDEX	70

# **ABOUT THIS HELP**

This document is a Kaspersky Rescue Disk deployment, customization and usage guide. The document is aimed at a wide range of users. Users should be able to use the computer at the beginner's level as a minimum: be familiar with the Microsoft Windows operating system interface and the basic methods of working with it and be able to use common applications.

The document is designed to:

- help user start up Kaspersky Rescue Disk and configure the application based on specific user tasks;
- ensure fast information search for solving application issues;
- enumerate alternative sources of information about the application and about ways of receiving technical support.

#### IN THIS SECTION:

In this document	6
	<u></u>
Legend	7

# IN THIS DOCUMENT

The Kaspersky Rescue Disk User Guide contains information on how to load, configure and work with Kaspersky Rescue Disk.

The following sections are included in the document:

## Additional sources of information

The section contains information on additional sources of data about the application and Internet resources where you can discuss the application, share new ideas, ask questions and receive comprehensive help.

# **Kaspersky Rescue Disk**

The section contains the description of the application's new features as well as brief information on its main features. Here you can find the hardware and software requirements which the computer should meet to be able to load Kaspersky Rescue Disk.

## Writing Kaspersky Rescue Disk to a removable drive

This section describes in detail how to write Kaspersky Rescue Disk to a removable drive.

## **Loading Kaspersky Rescue Disk**

This section contains instructions which will allow you to download the application and prepare it for work with Kaspersky Rescue Disk.

## Working with Kaspersky Rescue Disk in graphic mode

The section describes Kaspersky Rescue Disk operating mode in the graphic environment. The section contains information about the Anti-Virus interface, installation and shutdown, embedded applications and additional features of Kaspersky Rescue Disk. Here you can find information on computer protection, how to scan objects for viruses and update anti-virus databases on your computer. Here you can find information about the Quarantine, Backup, reports and how to work with them. The section also describes how to configure Kaspersky Rescue Disk.

## Working with Kaspersky Rescue Disk in text mode

This section describes how to work with Kaspersky Rescue Disk in text mode using the Midnight Commander file manager. It involves such issues as how to scan objects for viruses and update anti-virus databases on your computer. The information on network configuration is represented here.

#### **Hardware information**

This section describes how to save information on your system's hardware in electronic form for subsequent transfer to Kaspersky Lab.

### Restrictions in the application operation

This section describes the restrictions imposed on the operation of the Kaspersky Rescue Disk.

# **Contacting the Technical Support Service**

The section contains recommendations on how to get support in My Kaspersky Account on the Kaspersky Lab technical support website and by phone. This section also includes the recommendations on how to create and save the trace file.

### Glossary

The section contains a list of terms which are included in the document and their definitions.

#### Kaspersky Lab ZAO

The section contains information about the Kaspersky Lab software manufacturer. It also contains the description of other applications and the company contact information.

#### Information on third-party code

The section contains information on third-party code used when creating the application.

# **LEGEND**

The manual uses the legend specified below.

Table 1. Legend

TEXT EXAMPLE	LEGEND DESCRIPTION
Note that	Warnings are highlighted in red and enclosed in frames. Notifications contain important information connected with critical actions related to computer security.
You are advised to use	Notes are enclosed in frames. The notes contain support and background information.
Example:	The examples are given in the section below the Example heading on a yellow background.
Update – is	New terms are marked by italics.
ALT+F4	Names of keyboard keys are marked by semi-bold font and capital letters.
	The key names connected with the "plus" (+) character define a key combination.
Enable	Names of interface components, for example, input fields, menu commands, buttons, etc., are marked by semi-bold font.
To configure task schedule:	Instructions are marked by the arrow symbol.
-	The opening sentences or instructions are in italics.
help	Texts of the command line or texts of messages displayed on the screen have a special font.
<your address="" computer's="" ip=""></your>	The variables are enclosed in angle brackets. Instead of a variable its corresponding value is placed in every case, and the angle brackets are omitted.

# **ADDITIONAL SOURCES OF INFORMATION**

If you have any questions about the purchase, installation or use of Kaspersky Rescue Disk, answers are readily available.

Kaspersky Lab provides various sources of information about the application. You can choose the most suitable of them according to how important and urgent the question is.

#### IN THIS SECTION:

Sources of information to research on your own	<u>9</u>
Discussing Kaspersky Lab applications on the web forum	. <u>10</u>
Contacting the User documentation development group	. 10

# **SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN**

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

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

#### Application page at the Kaspersky Lab website

On the page <a href="http://www.kaspersky.com/removaltools">http://www.kaspersky.com/removaltools</a> you can get general information about Kaspersky Rescue Disk, its features and options.

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

On the page <a href="http://support.kaspersky.com/viruses/rescuedisk">http://support.kaspersky.com/viruses/rescuedisk</a> you will find articles by Technical Support Service specialists.

These articles contain useful information, recommendations and the Kaspersky Rescue Disk FAQ.

# **Help system**

Help contains information on how to manage computer protection: view protection status, scan various computer areas for viruses, execute other tasks.

To open Help, use the **Help** link.

If you have any questions regarding a separate Kaspersky Rescue Disk tab or window, you can use the context help.

To open context help, use the **Help** button or the **<F1>** key. The context help opens in the application window.

#### **Documentation**

The Kaspersky Rescue Disk User Guide contains detailed information required for working with the application.

# DISCUSSING KASPERSKY LAB APPLICATIONS ON THE WEB FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab's specialists and other users in our forum at <a href="http://forum.kaspersky.com">http://forum.kaspersky.com</a>.

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

# CONTACTING THE USER DOCUMENTATION DEVELOPMENT GROUP

If you have any questions about the documentation, or you have found an error in it, or would like to leave a comment, please contact our User documentation development group.

To do this, send a message with the subject "Kaspersky Help Feedback: Kaspersky Rescue Disk" to the email of the user documentation development group – <a href="mailto:documentation-development">docfeedback@kaspersky.com</a>.

# **KASPERSKY RESCUE DISK**

Kaspersky Rescue Disk is designed to scan and disinfect x86 and x64-compatible computers that have been infected. The application should be used when the infection is at such level that it is impossible to disinfect the computer using anti-virus applications or malware removal utilities (such as Kaspersky Virus Removal Tool) running under the operating system. In this case, disinfection is more efficient because malware programs do not gain control when the operating system is being loaded.

In system rescue mode only object scans and database updates are available as well as update rollback and viewing of statistics. You can take the following steps:

- Specify the virus scan task settings (see section "About object scan settings" on page 44):
  - change security level (see section "Changing security level" on page 46);
  - change actions to be performed on detected objects (see section "Changing actions to be performed on detected objects" on page 46);
  - create list of objects to be scanned (see section "Creating a list of objects to scan" on page 28);
  - change type of objects to scan (see section "Changing the type of objects to scan" on page 47);
  - restrict scan duration (see section "Restricting scan duration" on page 48);
  - specify settings for scanning compound files (see section "Scan of compound files" on page 48);
  - change the scan method (see section "Changing the scan method" on page 49);
  - restore default scan settings (see section "Restoring default scan settings" on page 50).
- Specify update task settings (see section "Disabling notifications" on page 59):
  - select update source (see section "Selecting an update source" on page <u>51</u>);
  - edit the proxy server settings (see section "Configuring proxy server settings" on page <u>52</u>);
  - specify regional settings (see section "Regional update source settings on page <u>52</u>);
  - roll back last update if necessary (see section "Rolling back the last update" on page 31).
- Configure additional settings (see section "Advanced application settings" on page 44):
  - select categories of threats to detect (see section "Selecting the detectable threat categories" on page 54);
  - create trusted zone (see section "Creating a trusted zone" on page 55);
  - configure notification settings (see section "About notification settings" on page <u>58</u>);

- specify storage time for report files (see section "Storing reports" on page 61);
- specify a storage setting for quarantined and backup objects (see section "Storing Quarantine and Backup objects" on page 62).
- Create report of scan and update tasks (see section "About reports" on page <u>35</u>).
- View application operation statistics (see section "About reports" on page <u>35</u>).

#### IN THIS SECTION:

What's new	. 12
Hardware and software requirements	. <u>12</u>

# **WHAT'S NEW**

Let us take a closer look at the new Kaspersky Rescue Disk features:

- Autorun objects can be disinfected.
- A heuristic analyzer has been added.
- The program modules have been updated.
- RAID arrays support has been added.
- The ability to configure a network, including Wi-Fi, has been added.
- Text mode operation has been modified.
- The operating system loader has been modified.
- The operating system kernel has been modified.
- The third-party application packages have been updated.
- A set of third-party application packages has been added.

# **HARDWARE AND SOFTWARE REQUIREMENTS**

For Kaspersky Rescue Disk to run properly, a computer should meet the following minimum requirements.

- General requirements:
  - CD-ROM / DVD (to install Kaspersky Rescue Disk from the installation CD).
  - USB socket (to install Kaspersky Rescue Disk from a removable boot drive).
  - Writing CD-ROM / DVD (for writing Kaspersky Rescue Disk image).
  - Support for booting from USB and CD / DVD.
  - Support for file systems FAT32/NTFS/Ext2/Ext3/Ext4/Reiser.
  - VESA-compatible video card.
- Microsoft Windows XP Home Edition (Service Pack 2 or higher), Microsoft Windows XP Professional (Service Pack 2 or higher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 or higher):
  - Intel Pentium 300 MHz processor or higher (or a compatible equivalent).
  - 256 MB free RAM.
- Microsoft Windows Vista Home Basic (32/64 bit), Microsoft Windows Vista Home Premium (32/64 bit), Microsoft Windows Vista Business (32/64 bit), Microsoft Windows Vista Enterprise (32/64 bit), Microsoft Windows Vista Ultimate (32/64 bit):
  - Intel Pentium 800 MHz 32 bit (x86)/ 64 bit (x64) processor or higher (or a compatible equivalent).
  - 512 MB free RAM.
- Microsoft Windows 7 Starter (32/64 bit), Microsoft Windows 7 Home Basic (32/64 bit), Microsoft Windows 7 Home Premium (32/64 bit), Microsoft Windows 7 Professional (32/64 bit), Microsoft Windows 7 Ultimate (32/64 bit):
  - Intel Pentium 1 GHz 32 bit (x86)/ 64 bit (x64) processor or higher (or a compatible equivalent).
  - 1 GB free RAM (32 bit); 2 GB free RAM (64 bit).

# WRITING KASPERSKY RESCUE DISK TO A REMOVABLE DRIVE

This section describes how to write Kaspersky Rescue Disk onto a removable drive.

You can write Kaspersky Rescue Disk quickly and easily using Kaspersky Anti-Virus 2011 and Kaspersky Internet Security 2011. These applications include a special service which allows creating and writing a rescue disk.

### IN THIS SECTION:

Preparing to write	. <u>14</u>
Writing Kaspersky Rescue Disk	14

# PREPARING TO WRITE

Kaspersky Rescue Disk can write an .iso image to a CD / DVD or to a removable drive. To write Kaspersky Rescue Disk, format your removable drive in the **Fat16**, **Fat32** or **NTFS** file system and make it a boot drive.

Even on small capacity USB drives, formatting takes some time (the larger the capacity, the longer the scan takes). Wait until formatting is finished.

To make a removable booting drive, use the corresponding applications (for instance, for Microsoft Windows XP you can use the **Diskpart** application and for Microsoft Windows Vista / Microsoft Windows 7 use the **HP USB Disk Storage Format Tool**).

# WRITING KASPERSKY RESCUE DISK

- To write a Kaspersky Rescue Disk image to a removable media:
  - 1. Load the Kaspersky Rescue Disk .iso image from the Kaspersky Lab server.
  - 2. Create a folder with the **rescue** name on your removable drive.
  - Copy the rescue.iso image to your removable drive (<Removable drive>:\rescue) and rename it to rescueusb.iso.
  - 4. Open the rescueusb.iso image with any .iso image editors (for instance, UltralSO).
  - 5. Copy the following files to your removable drive (<Removable drive>:\rescue) from the rescueusb.iso image:
    - README.txt.
    - the **help** folder.
  - 6. Copy the livecd file from the **rescueusb.iso** image to your removable drive (<Removable drive>:\) (rename to liveusb before copying).
  - 7. Modify the **boot\_from\_hard.cfg** content, located in the iso image under the following path: **boot \ grub \ cfg**.

    To do this, select the file and right-click it to open the menu and select the **Open with** option. In the window that

opens, select the **Select an application from the list manually** option. Click the **OK** button. Select the **Notepad** application and click the **OK** button. In the file that opens, replace **root (hd0)** with **root (hd1)**. Save changes.

The **boot\_from\_hard.cfg** content should be modified when working with Kaspersky Rescue Disk written to a removable drive. It is essential for an operating system correct boot from hard drive.

For some hardware and software configurations booting from hard drive is not available. In this case, remove your removable drive from the USB socket, reboot and make sure that in BIOS settings the hard drive with operating system is specified as a boot device.

- 8. Delete everything, except the **boot** folder, from the **rescueusb.iso** image. Save changes.
- 9. Copy the original **rescue.iso** image to <Removable drive>:\rescue. Now you have two .iso images on the removable drive: **rescueusb.iso** and **rescue.iso**.

**Rescueusb.iso** is used only for loading grub2 and booting Linux.

- 10. Click the <a href="http://nufans.net/grub4dos/grub4dos-0.4.4-2009-10-16.zip">http://nufans.net/grub4dos/grub4dos-0.4.4-2009-10-16.zip</a> link to download an archive. Unpack it to the corresponding folder. Open the unpacked folder.
- 11. Copy the following files from the specified folder to the root of your removable drive:
  - grldr.
  - menu.lst.

Modify the **menu.lst** content. To do this, select the file and right-click it to open the menu and select the **Open with** option. In the window that opens, select the **Select an application from the list manually** option. Click the **OK** button. Select the **Notepad** application and click the **OK** button. Replace all the file content with the following expression, following the syntax strictly:

```
map (hd0,0)/rescue/rescueusb.iso (0xff) || map --mem
(hd0,0)/rescue/rescueusb.iso (0xff)

map --hook
chainloader (0xff)
```

Save changes.

12. Obtain the number assigned to your removable disk.

To do this, in the task pane of your operating system select  $Start \rightarrow Control\ Panel \rightarrow Administrative\ Tools \rightarrow Computer\ management$ . In the window that opens, select  $Disk\ Management$  from the drop-down list. In the right part of the window a list of connected drives will open. Select your removable drive and remember its number.

- 13. Use the http://download.gna.org/grubutil/grubinst-1.1-bin-w32-2008-01-01.zip link to download an archive.
- 14. Open the command line. To do this, in the task pane of your operating system select the **Start** → **Run** and in the **Open** field enter **cmd**.
- 15. In the command line enter "Path to the downloaded archive\grubinst.exe" (hdN), where N is your disk number.

# **LOADING KASPERSKY RESCUE DISK**

This section contains instructions which will allow you to download the application and prepare it for work with Kaspersky Rescue Disk.

#### IN THIS SECTION:

Preparing to load	. <u>16</u>
Kaspersky Rescue Disk loading procedure	. 16

# PREPARING TO LOAD

- Before you load Kaspersky Rescue Disk:
  - 1. Enable booting from CD/DVD-ROM or a removable drive in BIOS settings (for more details please refer to the documentation for the motherboard installed on your computer).
  - 2. Insert a drive / removable drive into the CD/DVD-ROM drive with Kaspersky Rescue Disk image.
  - 3. Restart your computer. After reboot, a message will appear on the screen: Press any key to enter the menu.
  - 4. Press any key. A loading wizard will start.

If you do not press any key in 10 seconds, the computer boots from hard drive automatically.

# KASPERSKY RESCUE DISK LOADING PROCEDURE

- To continue loading Kaspersky Rescue Disk:
  - In the start up wizard window that opens, select the graphic interface language using the cursor moving keys. Click the ENTER button.

A window with various options will open.

- 2. Select one of the following start up methods:
  - Boot from Hard Disk.

For some hardware and software configurations booting from hard drive is not available. In this case, remove your removable drive from the USB socket, reboot and make sure that in BIOS settings the hard drive with operating system is specified as a boot device.

Kaspersky Rescue Disk. Graphic Mode loads the graphic subsystem.

 Kaspersky Rescue Disk. Text Mode loads the text user interface represented by the Midnight Commander (MC) console file manager.

You can also get and save information on the installed hardware (see section "Hardware information" on page <u>70</u>), start the computer from hard drive, restart or shut down the computer using the corresponding option from the list.

#### Click the ENTER button.

As a result, a Linux operating system will start up then the hardware will be detected and file systems on hard and removable drives will be searched for. The names used in the installed operating system are assigned to all file systems and removable drives.

If the loaded operating system is in sleep mode or its operation has been completed incorrectly, you will be asked to mount the file system or restart the computer. In this case select one of the three options:

- Continue. The application will continue mounting the file system, but there is a fairly high risk of file system damage.
- Skip. The application will skip file system mounting. Only boot sectors and autorun elements will be scanned.

Some file systems can be mounted.

Restart computer. This will allow you to boot from the hard drive to shut down the operating system
correctly.

The boot sequence is the following:

- a. Searching the Microsoft Windows swap file pagefile.sys. If it is missing, the volume of the virtual memory is limited by the RAM size.
- b. Creating the folders for anti-virus databases, reports, Quarantine and additional files.
- c. Network connections configuration based on data found in system files of the computer being loaded.
- d. The Anti-Virus starts if graphic mode was selected. The **Midnight Commander** file manager start with the opened user menu if text mode was selected.

# WORKING WITH KASPERSKY RESCUE DISK IN GRAPHIC MODE

This section describes Kaspersky Rescue Disk operating mode in the graphic environment.

#### IN THIS SECTION:

Kaspersky Rescue Disk interface	<u>18</u>
Starting and stopping Anti-Virus	<u>24</u>
Computer protection status	<u>25</u>
Objects scan	<u>27</u>
Jpdate	<u>30</u>
Quarantine and Backup	<u>32</u>
Reports	<u>35</u>
Advanced application settings	<u>44</u>
Closing Kaspersky Rescue Disk	<u>62</u>

# KASPERSKY RESCUE DISK INTERFACE

This section contains information on Anti-Virus interface and the additional features of Kaspersky Rescue Disk.

## IN THIS SECTION:

Taskbar	<u>18</u>
Anti-Virus interface	<u>19</u>
Additional tools	23

# TASKBAR

The taskbar is a panel displayed in the bottom part of the screen where the icon is displayed. Click the icon to open the Kaspersky Rescue Disk menu. You can also open the menu using the mouse. To do this, right-click any area on the desktop.

This opens the menu that provides quick access to the system elements (see the figure below).



Figure 1. Kaspersky Rescue Disk menu

The menu contains items which provide the following tools:

- Kaspersky Rescue Disk starts Anti-Virus.
- File manager (on page 23) starts X File Explorer (xfe) file manager.
- Web browser (on page <u>24</u>) starts Mozilla Firefox web browser.
- Terminal (on page <u>24</u>) starts operating system console.
- Screenshot (on page <u>24</u>) copies the screen as it is displayed on the monitor and indicates the path to the saved file.
- **Network setup** (on page 24) opens the network configuration window. In the window that opens, you can configure the network adapter and modify proxy server settings.
- About Kaspersky Rescue Disk opens the window containing information on Kaspersky Rescue Disk version.
- Restart computer opens the computer restart confirmation window.
- Shut down the computer opens the computer shutdown confirmation window.

You can also change the position of all the windows on the desktop. To do this, right-click the taskbar space to open the context menu and select the required action.

# **ANTI-VIRUS INTERFACE**

This section describes the main Anti-Virus features.

#### IN THIS SECTION:

Main window	. <u>20</u>
Configuration window	. <u>23</u>
Notifications	. 23

# **MAIN WINDOW**

The Kaspersky Rescue Disk main window is designed to implement all product features.

The main application window can be divided into two main parts:

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



There are three possible values of protection status (see section "Computer protection status" on page 25): each of them is indicated with a certain color, like stop lights. Green indicates that your computer's protection is at the correct level, while yellow and red indicate that there are various security threats. In addition to malicious programs, threats include obsolete application databases, protection settings are at minimum, etc.

Security threats must be eliminated as they appear. To obtain detailed information on threats and their elimination, click the status icon (see the figure above).

• The central part of the window can start an objects scan or an update using the corresponding tabs:

- On the **Objects Scan** tab (see the figure below) you can perform the following actions:
  - start / stop objects scan (see section "Starting and stopping the objects scan" on page 28);
  - add separate disks, directories, computer files to the scan task or delete them from the task (see section "Creating a list of objects to scan" on page 28);
  - view the process and results of the virus scan.



Figure 2. The Objects Scan tab

- On the **Update** tab (see the figure below) you can:
  - start / stop the update (see section "Starting and stopping the update" on page 31);
  - view the virus activity report, by clicking the corresponding link;
  - roll back databases to the previous version (see section "Rolling back the last update" on page 31);
  - · view update task progress and results.

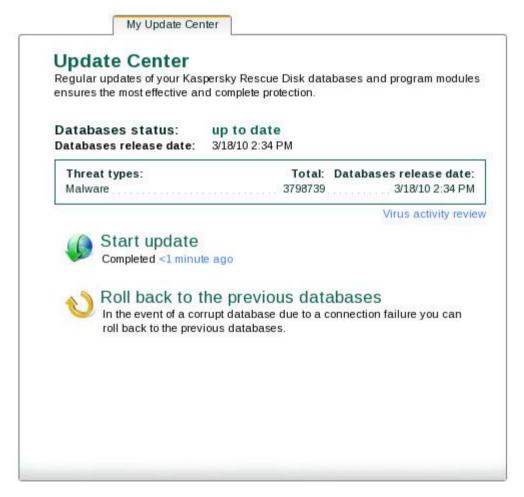


Figure 3. The Update tab

You can also use the following buttons and links:

- **Settings** to open the application settings window.
- Quarantine start working with quarantined objects.
- **Report** open the list of events occurring during application operation.
- **Help** view Kaspersky Rescue Disk help system.
- Exit stop Anti-Virus.

# **CONFIGURATION WINDOW**

You can open the Kaspersky Rescue Disk configuration window, by clicking the **Settings** link, located in the top part of the main application window. In this window you can configure the Kaspersky Rescue Disk settings.

The application settings window consists of two parts:

- the left part of the window ensures access to the object scans, updates, configuration settings of threats and exclusions, notifications and Kaspersky Rescue Disk reports and storages;
- the right part of the window contains a list of configurable settings in the left part of the section.

## **NOTIFICATIONS**

Whenever an event in the Kaspersky Rescue Disk operation occurs, a pop-up message is displayed on the screen.

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

- Alarm. A critical event has occurred; for instance, a virus has been detected. You should immediately decide
  how to deal with this threat. Notifications of this type are highlighted in red.
- Warning. A potentially dangerous event has occurred, for instance, a potentially infected object has been
  detected. You should decide on the degree of danger of this event. Notifications of this type are highlighted in
  yellow.
- Info. This notification gives information about non-critical events. Information notifications are highlighted in green.

# **ADDITIONAL TOOLS**

This section describes applications embedded in Kaspersky Rescue Disk and additional features of Kaspersky Rescue Disk.

#### IN THIS SECTION:

File manager	2 <u>23</u>
Web browser	<u>24</u>
Terminal	2 <u>24</u>
Screenshot	<u>24</u>
Network configuration	2 <u>24</u>

## **FILE MANAGER**

The integrated file manager **X** File Explorer (xfe) is based on the popular but currently undeveloped project X Win Commander. **X** File Explorer has a user-friendly interface and is effective when working with files for both advanced users and beginners.

Project home page: http://roland65.free.fr/xfe/

# **WEB BROWSER**

The Firefox web browser integrated in Kaspersky Rescue Disk can view websites and save the pages you have visited. You can view all visited pages after exiting Kaspersky Rescue Disk.

To access web pages via the integrated browser, a local network connection is required (Local Area Network connection). By default the web browser works with system proxy server. You can specify the proxy server settings when configuring the web browser. By default the Kaspersky Lab website is displayed in the browser.

## **TERMINAL**

The Terminal is an operating system console designed for working with command line in graphic mode.

# **SCREENSHOT**

This option can record the visual output displayed in the monitor and view the path to the saved file.

## **NETWORK SETUP**

This option can configure the network adapter and change the settings of the system proxy server. After the proxy server settings are modified, update retrieval and the browser will work with the proxy server settings that have been recently specified.

You can also specify the proxy server settings for an update task (see section "Configuring proxy server settings" on page 52) and for a web browser separately (see section "Web browser" on page 24).

# STARTING AND STOPPING ANTI-VIRUS

This section contains information on how to start and stop Anti-Virus.

#### IN THIS SECTION:

Starting Anti-Virus	24
Stopping Anti-Virus	<u>25</u>

# STARTING ANTI-VIRUS

- ➡ To run Anti-Virus, perform one of the following actions:
  - Right-click the space on the desktop, open the context menu and select 

    K Kaspersky Rescue Disk.
  - Click the icon located in the taskbar. In the menu that opens, select 
     Kaspersky Rescue Disk.

The Anti-Virus component starts after Kaspersky Rescue Disk starts up in graphic mode.

# **STOPPING ANTI-VIRUS**

- To stop Anti-Virus:
  - 1. Open the main application window and click the Exit button.

A dialog window with the following text will open on the screen: Are you sure want to exit **Kaspersky Rescue Disk?** 

2. Click the Yes button.

# **COMPUTER PROTECTION STATUS**

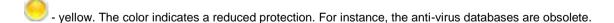
If your computer protection is threatened, its status will inform you. The protection icon changes its color (see figure below).



Figure 4. Current computer protection status

There are three possible values of protection status: each of them is indicated with a certain color like stop light colors:

- green. The color of this icon indicates that your computer is protected – the Kaspersky Rescue Disk databases have been updated in good time, the virus scan has not returned any malicious objects or malicious objects have been disinfected.



- red. The color indicates that there are problems which can result in the infection of your computer and loss of data: the application has not been updated for a long time, or malicious objects requiring urgent processing have been detected.

Security threats must be eliminated as they appear. You can view the list of problems, their description and troubleshooting suggestions on the **Status** tab (see the figure below), which you can select by double-clicking the status icon (see the figure above).

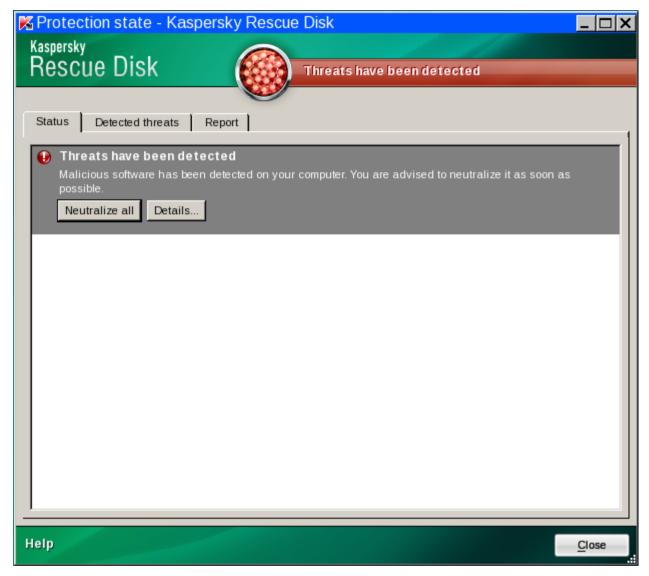


Figure 5. Solving security problems

The problems are listed based on their severity level: first are the most important ones, with red status icon, then less important ones (yellow status icon), the last ones are informational messages with the green status icon. Each problem is provided with its detailed description.

For the **Threats have been detected** problem the following options are available:

- Neutralize all. Click the Neutralize all button to fix the problem, which is the recommended action.
- Details. Click the Details button to go the Detected threats tab, where you can view the detailed information
  on the detected threat.

For the **Databases are out of date** the following options are available:

• Update now. Click the Update now button to go to the Update tab, where you can run an update task.

To display the previously hidden messages in the common list in the **Some messages are hidden** section, click the **Restore hidden messages** button.

# **OBJECTS SCAN**

This section contains information on how to scan your computer for viruses using Kaspersky Rescue Disk.

#### IN THIS SECTION:

About scanning objects for viruses	<u>27</u>
Starting and stopping the objects scan	<u>28</u>
Creating a list of objects to scan	<u>28</u>

# **ABOUT SCANNING OBJECTS FOR VIRUSES**

Virus scan is one of the most important tools for protecting your computer. The virus scan detects the spread of any malicious code, which for some reason may not have been detected by the malware protection.

After the object scan task starts (see section "Starting and stopping the objects scan" on page 28), Kaspersky Rescue Disk scans the objects selected by the user. You can scan any object in the computer's file system.

By default, the following list of objects corresponds to the object scan. It includes boot sectors and files on logical drives. You can edit this list as necessary (see section "Creating a list of objects to scan" on page 28).

Logical drives which are not assigned a name in Windows will be displayed in the following way - sdbN, where N - is a number assigned to disk by Kaspersky Rescue Disk (see the figure below).



Figure 6. Logical drives which are not assigned a name in Windows

The objects scan requires its own specific set of settings, configured in the Kaspersky Rescue Disk interface by default. Kaspersky Lab considers these settings to be optimal and has combined them in the **Recommended** security level. If the preset level does not meet your needs, you can:

- change security level (see section "Changing security level" on page 46);
- specify the file types (see section "Changing the type of objects to scan" on page 47) to be scanned for viruses;
- restrict scan duration (see section "Restricting scan duration" on page 48);
- configure settings for scanning compound files (see section "Scan of compound files" on page 48);
- select the scan method (see section "Changing the scan method" on page <u>49</u>), which determines its thoroughness;
- specify an action to be performed on detected objects (see section "Changing actions to be performed on detected objects" on page <u>46</u>).

When configuring scan task settings, you can always return to the recommended settings (see section "Restoring default scan settings" on page 50).

The task process is displayed in the Kaspersky Rescue Disk main application window, on the **Objects Scan** tab under the name of the running task.

While the scan is running, information about its results is logged in a Kaspersky Rescue Disk report (the **Report** link in the top part of the window).

#### **SEE ALSO:**

About object scan settings ......44

# STARTING AND STOPPING THE OBJECTS SCAN

- To start an objects scan task:
  - 1. Open the main application window.
  - On the Objects Scan tab, click the Start Objects Scan button. If you need to stop the task, click the Stop Objects Scan button while it is in progress.

The progress and the results of the scan will be displayed in the window that opens.

#### **SEE ALSO:**

About scanning objects for viruses......27

# **CREATING A LIST OF OBJECTS TO SCAN**

- To create a list of objects to scan:
  - 1. Open the main application window.
  - 2. On the **Objects Scan** tab, perform the following actions:
    - Click the Add link. This will open the Select an object to scan window. Add an object to the list of objects to scan.

Click the **OK** button after you have added all the objects you need.

If the Include subfolders box is checked when you add an object, the scan will be performed recursively.

- To delete an object from the list, click the **Delete** link.
- To edit an object from the list, click the Edit link.

In addition to deleting objects from the list, you can also temporarily exclude them from the scan. To do this, select an object from the list and uncheck the box to the left of the object's name.

Objects which appear on the list by default cannot be edited or deleted.

If the scan scope is empty or it contains no selected objects, the on-demand scan task cannot be started.

#### **SEE ALSO:**

# **UPDATE**

This section contains information on how to update the anti-virus databases on your computer using Kaspersky Rescue Disk.

#### IN THIS SECTION:

About the update	<u>30</u>
Starting and stopping the update	<u>31</u>
Rolling back the last update	<u>31</u>

# **ABOUT THE UPDATE**

Keeping the application updated is a prerequisite for reliably protecting your computer. New viruses, Trojans, and malicious software emerge daily, so it is important to regularly update the application to keep your personal data constantly protected. Information about threats and neutralization methods is stored in Kaspersky Rescue Disk's databases, so timely updating is an essential part in maintaining reliable protection.

To update anti-virus databases, run the update task (see section "Starting and stopping the update" on page 31). While the task is running, Kaspersky Rescue Disk downloads the updates and installs them on your computer.

If the databases have become corrupted during the update process, you can roll back update (see section "Rolling back the last update" on page  $\underline{31}$ ). Prior to updating the databases, Kaspersky Rescue Disk creates a backup copy of them should you want to roll back to the previous version.

Kaspersky Rescue Disk is updated according to a preset combination of settings.

If the preset settings do not meet your needs, you can:

- Select another update source (see section "Selecting an update source" on page 51).
- Change update source regional settings (see section "Regional update source settings" on page 52).
- Specify the proxy server settings (see section "Configuring proxy server settings" on page 52);

The anti-virus databases need to be constantly updated. You can decide whether it is necessary to download updates based on its status on the **Update** tab of the main application window. On the tab the following settings are displayed:

- Database status (up to date, out of date or corrupted).
  - When selecting an update source (see section "Selecting an update source" on page <u>51</u>), the anti-virus databases on your computer are compared with those at the update source. If the databases on your computer differ from those on the update server, the application downloads only the incremental part of the updates.
- Release date and time.
- Number of database records and their composition.

For detailed information about events, which have occurred during the task, go to the update report (the **Report** link in the top part of the window). You can also see the virus activity overview at www.kaspersky.com by clicking the **Virus** activity review link.

_			
•	 $\Lambda$ I	00	•
-31		- <b>3</b> L	)=

About update se	ttinas	 51	
ibout update se	ttings	 51	

# STARTING AND STOPPING THE UPDATE

- To start an update:
  - 1. Open the main application window.
  - 2. On the **Update** tab, click the **Start update** button. If you need to stop the task, click the **Stop update** button while it is in progress.

In the window that opens, the progress and the results of the update will be displayed.

#### **SEE ALSO:**

About the update	. 30
------------------	------

# **ROLLING BACK THE LAST UPDATE**

- To roll back to the previous database version:
  - 1. Open the main application window.
  - 2. On the Update tab, click the Roll back to the previous databases button. A Rollback window will open.
  - 3. In the window that opens, click the Roll back the last update button.

## SEE ALSO:

About the update	

# **QUARANTINE AND BACKUP**

This section contains information on Quarantine and Backup.

#### IN THIS SECTION:

About Quarantine	<u>32</u>
Actions with quarantined objects	<u>33</u>
About Backup	33

# **ABOUT QUARANTINE**

Quarantine is a special repository that stores the objects which may be infected with viruses.

Potentially infected objects are objects that are suspected of being infected with viruses or their modifications. Such an object can be discovered and quarantined when scanning for viruses.

Objects are guarantined when scanning for viruses in the following cases:

• The code of the object being analyzed resembles a known threat but is partially modified.

The Kaspersky Rescue Disk databases contain the threats investigated to date by Kaspersky Lab specialists. If a malicious program is modified and these changes have not yet been entered into the databases, Kaspersky Rescue Disk classifies the object infected with the modified malicious program as a potentially infected object, and indicates without fail what threat this infection resembles.

• The code of the object detected has a structure like a malicious program; however, nothing similar is recorded in the application databases.

It is quite possible that this is a new type of threat, so Kaspersky Rescue Disk classifies the object as a potentially infected object.

Files are identified as potentially infected with a virus by the heuristic code analyzer. This mechanism is fairly effective and rarely leads to false positives.

When you place an object in Quarantine, it is moved, not copied: the object is deleted from the disk, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous. You can modify Quarantine settings (see section "Storing Quarantine and Backup objects" on page 62).

You can perform the following actions on the quarantined objects:

- quarantine the files that you suspect are infected;
- scan and disinfect using the current Kaspersky Rescue Disk databases;
- restore files to the folders from which they were moved to Quarantine, or to the folders selected by the user;
- delete any quarantined object or group of selected objects.

You can modify an action to be performed on quarantined objects (on page 33).

#### **SEE ALSO:**

Storing Quarantine and Backup objects......<u>62</u>

# **ACTIONS WITH QUARANTINED OBJECTS**

- To perform actions on quarantined objects:
  - 1. Open the main application window.
  - 2. Click the Quarantine link in the top part of the window. This will open the Protection state window.
  - 3. In the window that opens, on the **Detected threats** tab, select an object and right-click to open its context menu.
  - 4. Select an action to be performed on the object:
    - Scan scan all quarantined objects.
    - **Delete from the list** remove the object detection record from the list. After the object is removed from the list, it is deleted from Backup.
    - Restore restore the object.
    - Disinfect all neutralize all objects on the list. The application will attempt to process the objects using the
      anti-virus databases.

This action is only available for active threats.

 Clear list – clear the list of detected objects. You will be invited to delete the objects from the list and from the Backup.

You cannot delete the objects only from the list.

### **SEE ALSO:**

About Quarantine 32

# **ABOUT BACKUP**

Sometimes the integrity of objects cannot be maintained during disinfection. If the disinfected file contained important information, and after disinfection it became fully or partially inaccessible, you can attempt to restore the original object from its backup copy.

Backup copy is a copy of the original dangerous object that is created when first disinfecting or deleting the object, and it is saved in backup.

*Backup* is a special repository that contains backup copies of dangerous objects after processing or deletion. The main function of a backup storage is the ability to restore the original object at any time. Files in backup are saved in a special format and are not dangerous. You can modify the settings of storing backup objects (see section "Storing Quarantine and Backup objects" on page 62).

## **SEE ALSO:**

Storing Quarantine and Dackup objects	tine and Backup objects6	2
---------------------------------------	--------------------------	---

# **REPORTS**

This section contains information on reports and how to work with them.

#### IN THIS SECTION:

About reports	<u>35</u>
Selecting task to create a report	3 <u>6</u>
Managing information grouping in the report	3 <u>6</u>
Selecting event type	<u>37</u>
Displaying data on the screen	<u>38</u>
Saving report to a file	<u>40</u>
Using complex filtering	<u>41</u>
Events search	<u>42</u>
Extended statistics display	<u>43</u>

# **ABOUT REPORTS**

All object scans and updates are logged in a report. It displays the number of dangerous and suspicious objects detected by the application in the specified period.

While working with reports you can perform the following actions:

- Select a task (see page <u>36</u>) you want to view event report of.
- Manage data group (see page <u>36</u>).

You can manage the data group represented in the report. The information can be grouped by a number of attributes.

Select the event type (see page <u>37</u>) for which the report should be generated.

A full list of important events that occur when running the scan task or updating the databases, is displayed in the report. You can select which type of events will be recorded in the report.

Manage data displayed on the screen (see page 38).

Events included in the report will be displayed as a table. You can create a dataset to filter the information, by specifying a restricting condition.

Select how the statistical information will be displayed (see page 43) on the screen.

In the bottom part of the window the Kaspersky Rescue Disk tasks statistics is displayed.

Save the report in a file (see page <u>40</u>).

• Specify complex filtering conditions (see page 41).

You can specify data search criteria for any table column. A data query using a complex filter is based on the logical conjunction (Logical **And**) function and disjunction (Logical **Or**) function which can be used to control the query.

Search for events (see page 42) which occurred in the system and were processed by the application.

The objects scan and update operation is logged in the statistics section (see section "Extended statistics display" on page 43). You can review the extended statistics in graphic form or in table view (depending on the task). The extended

statistics is selected using the button in the top part of the window. Here you can check how many hazardous and suspicious objects have been detected by the application, and which ones were disinfected, deleted or quarantined.

#### **SEE ALSO:**

Reports and storages 59

# SELECTING TASK TO CREATE A REPORT

- To obtain the report of a task:
  - 1. Open the main application window.
  - 2. Click the Report link in the top part of the window. This will open the Protection state window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
  - In the window that opens in the drop-down list located in the top left corner, select a task for which a report should be created (see the figure below).



Figure 7. Selecting task to create a report

#### **SEE ALSO:**

## Managing information grouping in the report

- In order to use grouping based on a certain attribute:
  - 1. Open the main application window.
  - 2. Click the Report link in the top part of the window. This will open the Protection state window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
  - 4. Select the grouping attribute from the drop-down list (see the figure below) in the window that opens:
    - Do not group the events will not be grouped.
    - Group by result data will be grouped based on the results of scan or object processing.

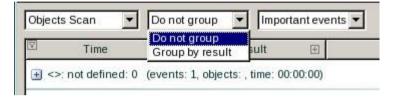


Figure 8. Selecting a filter

To quickly obtain particular information and to decrease the grouping size, a keyword search criterion is provided (see section "Events search" on page  $\underline{42}$ ). You can also specify a search criterion.

## SEE ALSO:

## **SELECTING EVENT TYPE**

- In order to create a report about a particular event type:
  - 1. Open the main application window.
  - 2. Click the **Report** link in the top part of the window. This will open the **Protection state** window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

- 4. In the window that opens from the drop-down list on the right (see the figure below), select the event type:
  - Critical events events of a critical importance which indicate problems with Kaspersky Rescue Disk, or vulnerabilities in the protection of your computer. They include, for instance, detection of a virus or an operation failure.
  - **Important events** events which should always be attended to since they reflect important situations in the application's operation, for example, the **terminated** event.
  - All events if a report on all events needs to be created.



Figure 9. Selecting event type

If you select **All events**, the report will display all events but only if in the **Reports and Storages** section, in the **Reports** group of fields the corresponding box is checked (see section "Logging non-critical events in a report" on page <u>61</u>). This parameter allows the non-critical report logs to be included in the report. If this box is not checked, a warning icon and the **Disabled** link are displayed near the event type selection dropdown list. Click the specified link to open the reports configuration window and check the corresponding boxes.

#### **SEE ALSO:**

About reports

## DISPLAYING DATA ON THE SCREEN

- To modify the data displayed on the screen:
  - 1. Open the main application window.
  - 2. Click the Report link in the top part of the window. This will open the Protection state window.

- 3. In the window that opens, on the Report tab click the Detailed report button and configure the displayed data:
  - To impose a restriction, left-click the area to the left of the heading of the table column for which you wish to impose a restriction (see the figure below). Select a required restriction from the drop-down list. If Custom is selected, you can specify complex filtering conditions (see section "Using complex filtering" on page 41). If necessary, you can view all data by selecting All in the restrictions list.

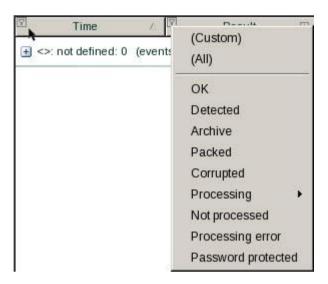


Figure 10. Specifying a restricting condition

• To view detailed information about an event, click the 🗈 icon located on the left of the event header. You can change the way that data are displayed on the screen. To do this, right-click the area on the right of any column header and in the context menu define the filter (see the figure below).

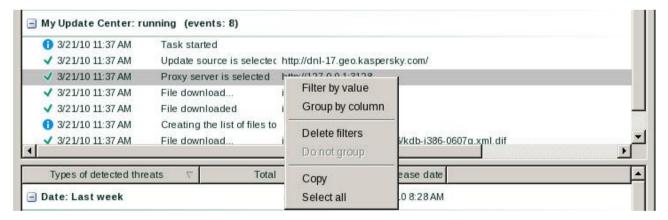


Figure 11. Selecting the data display mode

• In order to hide / show table columns, in the window that opens, right-click the area to the right of the heading of any table column and uncheck the boxes with corresponding names in the context menu (see the figure below).

• The context menu of the column provides quick access to any attribute which allows grouping and selecting events (see the figure below).

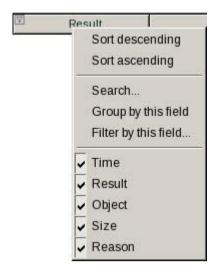


Figure 12. Grouping and event querying menu

• To display all items in the table columns, click the button ■, located to the left of the required column name (see the figure below). In the opened columns headers an arrow is displayed which indicates the filter order. You can modify the filter by clicking the arrow icon.

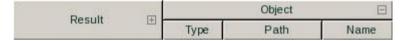


Figure 13. Displaying complete table columns

## SEE ALSO:

About reports 35

## SAVING REPORT TO A FILE

- To save the obtained report into a file:
  - 1. Open the main application window.
  - 2. Click the Report link in the top part of the window. This will open the Protection state window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button. As a result, a correspondingly named window will open.
  - 4. Create the required report and click the **Save** button.
  - 5. Select a folder in which the report file should be logged and enter the file name.

#### **SEE ALSO:**

## **USING COMPLEX FILTERING**

- To specify complex filtering conditions:
  - 1. Open the main application window.
  - 2. Click the Report link in the top part of the window. This will open the Protection state window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button. As a result, a correspondingly named window will open.
  - 4. Left-click the area to the left of the table column for which you wish to specify complex filtering conditions. In the window the opens, select **Custom** (see the figure below). You can also select **Filter by this field** in the context menu (see section "Displaying data on the screen" on page 38) displayed after right-clicking the necessary column of the table.

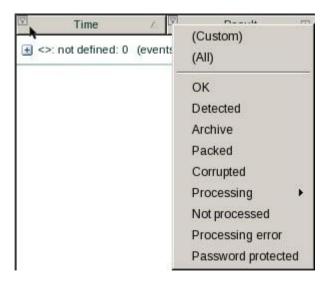


Figure 14. Specifying a restricting condition

5. In the Custom filter window that opens specify the necessary filtering conditions.

The query limits are specified in the fields in the right part of the window. The left part of the drop-down list **Show rows where** is used to pick the condition for events query (for example, is greater than, i.e. exceeding the value specified in the field to the right).



Figure 15. Specifying the complex filtering conditions

If you wish your data query to satisfy both specified conditions, select **And**. If only one of the two conditions is required, select **Or**.

For several types of columns the search interval limit is not a numeric or a temporal value, but a word (for example, the query could pick out the **OK** value for the **Result** column). In this case the word specified as the limit will be compared against other word-conditions in alphabetic order.

## **SEE ALSO:**

About reports 35

## **EVENTS SEARCH**

- To use events search:
  - 1. Open the main application window.
  - 2. Click the **Report** link in the top part of the window. This will open the **Protection state** window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button.

- 4. In the window that opens, right-click the area to the right of the heading of any table column. Select **Search** from the context menu.
- 5. In the **Search** window that opens (see the figure below), specify the search criteria.



Figure 16. Search window

#### **SEE ALSO:**

## **EXTENDED STATISTICS DISPLAY**

- To view the extended statistics:
  - 1. Open the main application window.
  - 2. Click the Report link in the top part of the window. This will open the Protection state window.
  - 3. In the window that opens, on the **Report** tab, click the **Detailed report** button.
  - 4. In the window that opens, select a task for which you want to view the extended statistics and click the button in the top part of the window.

## **SEE ALSO:**

## **ADVANCED APPLICATION SETTINGS**

This section includes information on how to configure Kaspersky Rescue Disk.

## IN THIS SECTION:

Objects scan	44
Update	
Threats and exclusions. Trusted zone	<u>53</u>
Notifications	57
Reports and storages	59

## **OBJECTS SCAN**

This section contains information on how to configure the objects scan settings on your computer.

## IN THIS SECTION:

About object scan settings	<u>44</u>
Changing security level	<u>46</u>
Changing actions to be performed on detected objects	<u>46</u>
Changing the type of objects to scan	<u>47</u>
Restricting scan duration	<u>48</u>
Scan of compound files	<u>48</u>
Changing the scan method	<u>49</u>
Restoring default scan settings	50

## **ABOUT OBJECT SCAN SETTINGS**

The method to be used to scan objects on your computer is selected by the settings assigned for this task.

To configure the objects scan:

Change security level (see section "Changing security level" on page 46);

The security level is a preset collection of scan settings. Kaspersky Lab specialists distinguish three security levels:

- High most complete scan of the entire computer or individual disks, folders, or files.
- Recommended the same objects are scanned as at the High level, except email format files.
- Low a level requiring less RAM resources, since the set of files to be scanned is reduced.

You should select the level based on your own preferences.

Specify the file types (see section "Changing the type of objects to scan" on page 47) to be scanned for viruses.

By default Kaspersky Rescue Disk scans only potentially infectable files. You can widen or restrict the protection scope by changing the type of files to be scanned. For example, you wish to scan only .exe files run from removable drives. However, you should make sure that you do not expose your computer to the threat of infection when narrowing down the protection scope.

Restrict scan duration (see section "Restricting scan duration" on page 48).

You can set a restriction on the duration of the scan for each file. The scan of such a file will be stopped after the specified time.

Specify settings for scanning compound files (see page <u>48</u>).

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

You can specify the type of compound files to be scanned. You can also specify a maximum size for a compound file to be scanned. Compound files larger than the specified value will not be scanned.

 Select the scan method (see section "Changing the scan method" on page <u>49</u>), which determines its thoroughness.

You can edit the scan settings to determine its thoroughness. By default, the mode of using the application's database records to search for threats is always enabled.

The databases are created by Kaspersky Lab experts. They contain a detailed description of all currently existing threats to computer security as well as methods used for detection and disinfection. Kaspersky Lab constantly updates the databases as new threats appear. In order to achieve higher quality threat detection we recommend that you update databases from Kaspersky Lab's update servers on a regular basis.

The scan mode in which Kaspersky Rescue Disk compares the object found with the database records is called *signature analysis* and is always used. You can also use *heuristic analysis*. This method consists of the analysis of the actions an object performs within the system. If these actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious.

You can also select the detail level for heuristic analysis: **light**, **medium**, or **deep**. To do this, move the slider bar to the selected position.

 Specify an action to be performed on detected objects (see section "Changing actions to be performed on detected objects" on page 46).

If a threat is detected, Kaspersky Rescue Disk assigns it one of the following statuses:

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

Kaspersky Rescue Disk will notify you if it detects infected or potentially infected objects during a virus scan. You should react to an emerging threat by selecting an action to be performed on the object. Kaspersky Rescue Disk selects the **Prompt when the scan is complete** option as the action on a detected object which is the default setting. You can change the action.

Restore the recommended settings (see section "Restoring default scan settings" on page 50).

Kaspersky Lab considers these settings to be optimal and has combined them in the **Recommended** security level.

#### SEE ALSO:

About scanning objects for viruses......27

## **CHANGING SECURITY LEVEL**

- To change the defined security level:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. This opens the **Objects Scan** section.
  - 3. In the **Security level** section select the required security level:
    - **High** complete scan of the entire computer or individual disks, folders, or files.
    - Recommended the same objects are scanned as at the High level, except email format files.
    - Low a level requiring less RAM resources, since the set of files to be scanned is reduced.

If none of the preset levels meets your needs, you can configure the scan settings yourself. The security level will then be changed to **Custom**. To restore the default scan settings, select one of the preset security levels or click the **Default** button.

## SEE ALSO:

## **CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS**

Before disinfecting or deleting an object, Kaspersky Rescue Disk creates a backup copy and places it in backup against a future need to recover or disinfect the object if that should become possible.

- ▶ To change the specified action to be performed on detected objects:
  - 1. Open the main application window.
  - 2. Click the Settings link in the top part of the window. This opens the Objects Scan section.
  - 3. In the **Action** section select one of the following:
    - **Prompt when the scan is complete** Kaspersky Rescue Disk will postpone processing of objects until the scan is complete.
    - Prompt on detection the application displays a warning message containing the information about which
      malicious code has penetrated the infected / potentially infected object, and offers a choice of further
      actions.
    - Select action:
      - **Disinfect** Kaspersky Rescue Disk attempts to disinfect the object without requesting user confirmation. Potentially infected objects are placed to Quarantine. Relevant information is logged in the report. Later you can attempt to disinfect this object.
      - Delete if disinfection fails Kaspersky Rescue Disk attempts to disinfect the object without requesting confirmation. Incurable objects are deleted, potentially infected objects are moved to Quarantine.

#### SEE ALSO:

## **CHANGING THE TYPE OF OBJECTS TO SCAN**

- To change the type of objects to be scanned:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. This opens the **Objects Scan** section.
  - 3. In the Security level section click the Settings button.

- 4. In the window that opens, on the **Scope** tab, in the **File types** section, specify the format and extension of the files that are to be scanned when the selected scan task runs:
  - All files with this option, all files will be scanned without exception.
  - Files scanned by format if you select this group, Kaspersky Rescue Disk will scan only potentially infected files, i.e. files which a virus could infiltrate. Before searching for viruses in an object, its internal header is analyzed to determine the file format (.txt, .doc, .exe, etc.).
  - **Files scanned by extension** in this case Kaspersky Rescue Disk will only scan potentially infected files. The file format will be determined by its extension.

Please remember that the probability of malicious code penetrating files of certain formats (for example, .txt) and subsequent activation is quite low. At the same time the risk of malicious code penetrating files that contain or may contain executable code (for instance, .exe, .dll, .doc), is quite high.

Remember that an intruder can send a virus to your computer in a file with the .txt extension, whereas it is in fact an executable file renamed as .txt file. If you select the **Files scanned by extension** option, the scan would skip this file. If the **Files scanned by format** option has been selected, the file protection will analyze the file header and determine that the file is an .exe file. Such a file will be thoroughly scanned for viruses.

#### **SEE ALSO:**

About object scan settings .......44

## **RESTRICTING SCAN DURATION**

- To set a restriction on scan duration:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. This opens the **Objects Scan** section.
  - 3. In the Security level section click the Settings button.
  - 4. In the window that opens, on the Scope tab, in the Scan optimization section, check the 
    Skip files scanned longer than box and specify the scan duration in the field next to it. The file scan will be stopped after the specified time.

#### SEE ALSO:

## **SCAN OF COMPOUND FILES**

- To configure the settings to scan compound files:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. This opens the **Objects Scan** section.
  - 3. In the **Security level** section click the **Settings** button.
  - 4. In the window that opens, on the **Scope** tab in the **Scan of compound files** section, you can specify the following settings:
    - Type of compound files to be scanned. To do this, check the boxes next to the required items.
    - Maximum size of compound files to be scanned. To do this, click the Additional button. In the Compound files window that opens, check the Do not unpack compound files larger than box and specify the maximum file size in the field below. Compound files larger than this maximum size will not be scanned.

If the **Do not unpack large compound files** box is checked, and the size of the compound file does not exceed the defined maximum value, extracted files will be scanned even if their size exceeds the defined maximum value.

#### **SEE ALSO:**

About object scan settings ......44

## **CHANGING THE SCAN METHOD**

- To change the scan method:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. This opens the **Objects Scan** section.
  - 3. In the **Security level** section click the **Settings** button.

- 4. In the window that opens, select the **Additional** tab.
- 5. In the **Scan methods** section select the scan method:
  - Signature analysis. Signature analysis uses the Kaspersky Rescue Disk database, which contains
    descriptions of known threats and methods for eradicating them. Protection using signature analysis
    provides a minimal level of security. Following the recommendations of Kaspersky Lab's experts, this
    method is always enabled.
  - Heuristic analysis. The scan is based on the analysis of typical sequences of operations, allowing a
    reasonably certain conclusion about the nature of the file. The advantage of using this method is that new
    threats are detected before virus analysts have encountered them.

You can also set the detail level for scans: Light, Medium, or Deep. To do this, move the slider bar to the selected position.

## SEE ALSO:

## **RESTORING DEFAULT SCAN SETTINGS**

- ➡ In order to restore the default object scan settings:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. This opens the **Objects Scan** section.
  - 3. In the Security level section click the Default level button.

You can always restore the recommended object scan settings. Kaspersky Lab considers that these are optimal and has combined them in the **Recommended** security level.

## **SEE ALSO:**

## **UPDATE**

This section contains information on how to configure update settings on your computer.

#### IN THIS SECTION:

About update settings	<u>51</u>
Selecting an update source	<u>51</u>
Configuring proxy server settings	<u>52</u>
Regional update source settings	<u>52</u>

## **ABOUT UPDATE SETTINGS**

Kaspersky Rescue Disk update is carried out according to a group of settings.

To configure the update settings:

• Select an update source (see section "Selecting an update source" on page 51).

You must have an Internet connection to update.

A resource containing Kaspersky Rescue Disk database and module updates is called an *update source*. You can use HTTP or FTP servers as an update source. The main default update source is the Kaspersky Lab update servers located in several countries. These are special Internet sites where the updates for all Kaspersky Lab products are stored. If several resources are selected as update sources, Kaspersky Rescue Disk will try to connect to them in turn, starting at the top of the list and retrieving the updates from the first available source.

Change update source regional settings (see section "Regional update source settings" on page <u>52</u>).

Choosing the Kaspersky Lab update server closest to you will save you time and download updates faster. You can select the optimal server location when downloading updates.

• Specify the proxy server settings (see section "Configuring proxy server settings" on page 52);

To download updates from servers, your computer must be connected to the Internet. By default, the Internet connection settings are determined automatically. If you are using a proxy server, the connection settings (see section "Configuring proxy server settings" on page 52) should be set.

SEE ALSO:
-----------

About the undete		
About the update	 	 

## **SELECTING AN UPDATE SOURCE**

You must have an Internet connection to update.

- To choose an update source:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. In the left part of the window select the **Update** section.
  - 3. Click the **Settings** button in the right part of the window.
  - 4. Click the Add link on the Source tab in the displayed window. The Select update source window will open.
  - 5. In the window that opens, select an FTP or HTTP site, or enter its IP address, symbolic name or URL.

#### **SEE ALSO:**

## **CONFIGURING PROXY SERVER SETTINGS**

By default the update task works with the system proxy server. You can specify the proxy server settings for the update task separately.

- To configure the proxy server settings:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. In the left part of the window select the **Update** section.
  - 3. Click the **Settings** button in the right part of the window.
  - 4. In the window that opens, on the **Source** tab, click the **Proxy server** button.
  - 5. In the window that opens, specify the proxy server settings.

## SEE ALSO:

About update settings .......<u>51</u>

## **REGIONAL UPDATE SOURCE SETTINGS**

- To choose the closest server:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. In the left part of the window select the **Update** section.
  - 3. Click the **Settings** button in the right part of the window.
  - 4. In the window that opens, on the **Source** tab, in the **Regional** settings section, select from the drop-down list the **Select from the list** option. In the drop-down list, specify the country nearest to your current location.

## SEE ALSO:

About update settings .......<u>51</u>

## THREATS AND EXCLUSIONS. TRUSTED ZONE

This section contains information on how to protect your computer from various kinds of malware by expanding the list of detected threats, as well as information on how to exclude from the scan some most used applications and how to configure exclusion rules.

## IN THIS SECTION:

About threats and exclusions	<u>53</u>
Selecting the detectable threat categories	<u>54</u>
About trusted zone	<u>54</u>
Creating a trusted zone	<u>55</u>
Creating an exclusion rule	<u>56</u>
Allowed file exclusion masks	<u>56</u>
Verdict exclusion masks permitted according to Virus Encyclopedia	57

## **ABOUT THREATS AND EXCLUSIONS**

Kaspersky Rescue Disk protects you against various types of malware. Regardless of the settings selected, the application will always scan and disinfect viruses, Trojans and hacker utilities. These programs can significantly damage your computer. To make your computer more secure, you can expand the list of threats that the program will detect by enabling monitors for various potentially dangerous programs.

In the **Threats and exclusions** section of the Kaspersky Rescue Disk's settings window, you can perform the following actions:

- Select categories of threats to detect (see section "Selecting the detectable threat categories" on page 54).
- Create a trusted zone for the application (see section "Creating a trusted zone" on page 55).

*Trusted zone* (see section "*About trusted zone*" on page <u>54</u>) is a list of objects created by the user which Kaspersky Rescue Disk does not monitor. In other words, it is a set of exclusions from the protection scope.

The user manually creates a trusted zone based on the features of the objects he or she works with. You might need to create such an exclusion list if, for example, Kaspersky Rescue Disk blocks access to an object but you are sure that the object is absolutely safe.

#### **SEE ALSO:**

Threats and exclusions. Trusted zone ......53

## **SELECTING THE DETECTABLE THREAT CATEGORIES**

- ➡ To select the detectable threat categories:
  - 1. Open the main application window.
  - Click the Settings link in the top part of the window. In the left part of the window select the Threats and exclusions section.
  - 3. In the right part of the window, in the **Threats** section click the **Settings** button.
  - 4. In the **Threats** window that opens, check the boxes next to the threat categories that you want to protect your computer from.

## SEE ALSO:

About threats and exclusions ......53

#### ABOUT TRUSTED ZONE

*Trusted zone* is a list of objects created by the user which Kaspersky Rescue Disk does not monitor. In other words, it is a set of exclusions from the protection scope.

The user manually creates a trusted zone (see section "Creating a trusted zone" on page <u>55</u>) based on the features of the objects he or she works with. You might need to create such an exclusion list if, for example, Kaspersky Rescue Disk blocks access to an object but you are sure that the object is absolutely safe.

Trusted zone is created based on the exclusion rules (see section "Creating an exclusion rule" on page  $\underline{56}$ ). Exclusion rules are sets of conditions that Kaspersky Rescue Disk uses to verify if it can skip the scan of an object.

You can specify the grounds for excluding files from the scan:

• Object excludes a given object, directory, or files that match a certain mask from scans.

An exclusion object is not scanned when the disk or folder where it is located is scanned. However, if you select that object specifically, the exclusion rule will not be applied.

Threats type means excluding objects from the scan based on their status in the Virus Encyclopedia
classification. This status is assigned based on the classification of malware and riskware found in the
Kaspersky Lab Virus Encyclopedia.

Potentially dangerous software does not have a malicious function but can be used as an auxiliary component for a malicious code, because it contains holes and errors. This category includes, for example, remote administration programs, IRC clients, ftp services, all-purpose utilities for stopping processes or hiding them, keyloggers, password macros, autodialers, etc. These programs are not classified as viruses (not-a-virus). They can be subdivided into different types, such as Adware, Joke, Riskware, etc. (for more information on potentially malicious software detected by Kaspersky Rescue Disk, see the Virus Encyclopedia at www.viruslist.com). These programs may be blocked by the application. Since many of them are widely used, the possibility is provided to exclude potentially malicious programs from the scan. To do this, you must specify the verdict assigned to that program as an exclusion.

For example, you may frequently use a Remote Administrator program, which allows you to control a computer from a remote computer. Kaspersky Rescue Disk views this sort of application activity as potentially dangerous and may block it. To keep the application from being blocked, you must create an exclusion rule that specifies RemoteAdmin.

When an exclusion is being added, it results in a rule, which can be further used at the execution of virus scan.

#### SEE ALSO:

Creating a trusted zone .......55

#### CREATING A TRUSTED ZONE

- To create a trusted zone:
  - 1. Open the main application window.
  - Click the Settings link in the top part of the window. In the left part of the window select the Threats and exclusions section.
  - 3. In the right part of the window, in the Exclusions section click the Settings button.

- 4. In the window that opens, on the Exclusion rules tab:
  - Click the Add link. This opens the Exclusion rule window. In the window that opens, specify the exclusion rules.
  - To delete a rule from the list, click the **Delete** link.
  - Click the Edit link to modify the created rule.

As well as deleting rules from the list, you can also temporarily exclude them from the scan. To do this, select a rule from the list and uncheck the box to the left of its name.

#### SEE ALSO:

About trusted zone	5
--------------------	---

## **CREATING AN EXCLUSION RULE**

- To create an exclusion rule:
  - 1. Open the main application window.
  - Click the Settings link in the top part of the window. In the left part of the window select the Threats and exclusions section.
  - 3. In the right part of the window, in the **Exclusions** section click the **Settings** button.
  - 4. Click the Add link on the Exclusion rules tab in the displayed window. This opens the Exclusion rule window.
  - 5. In the window that opens, in the **Properties** section, specify the exclusion type.

#### **SEE ALSO:**

About threats and exclusions	
Anolit threate and evellicions	<b>5</b> .

## **ALLOWED FILE EXCLUSION MASKS**

Let's take a look at some examples of allowed masks that you can use when creating file exclusion lists:

- 1. Masks without file paths:
  - \*.exe all files with the .exe extension;
  - \*.ex? all files with the .ex? extension where ? can represent any single character;
  - \*test\* all files with the name test.
- 2. Masks with absolute file paths:
  - /discs/C:/dir/\*.\*, or /discs/C:/dir/\*, or /discs/C:/dir/ all files in the folder with the name /discs/C:/dir/;
  - /discs/C:/dir/\*.exe all files with the .exe extension in the folder with the name /discs/C:/dir/;

- /discs/C:/dir/\*.ex? all files with the .ex? extension in the /discs/C:/dir/ folder where? may represent any single character;
- /discs/C:/dir/test\* files in /discs/C:/dir/ folder, with names starting with test.

If you want the application to exclude files in all nested subfolders of the specified folder from a scan, check the **r** include subfolders box when creating the mask.

## 3. File path masks:

- dir/\*.\*, or dir/\*, or dir/ all files in all folders with dir/;
- dir/\*test\* all test files in folders with dir/;
- dir/\*.exe all files with the .exe extension in all folders with dir/;
- dir/\*.ex? all files with the .ex? extension in all dir/ folders where? may represent any single character.

If you want the application to exclude files in all nested subfolders of the specified folder from a scan, check the **Include subfolders** box when creating the mask.

\*.\* and \* exclusion masks can only be used if you assign an excluded threat verdict. In this case the specified threat will not be detected in any objects. Using these masks without selecting a verdict essentially disables monitoring.

## VERDICT EXCLUSION MASKS PERMITTED ACCORDING TO VIRUS ENCYCLOPEDIA

When adding threats with a certain verdict from Virus Encyclopedia classification as exclusions, you can specify the following information:

- the full name of the threat as given in the Virus Encyclopedia at www.viruslist.com (for example, not-a-virus:RiskWare.RemoteAdmin.RA.311 or Flooder.Win32.Fuxx);
- the threat name as a mask. For example:
  - not-a-virus\* exclude legal but potentially dangerous programs from the scan as well as joke programs;
  - \*Riskware.\* exclude all potentially dangerous riskware programs from the scan;
  - \*RemoteAdmin.\* exclude all versions of the remote administration program from the scan.

## NOTIFICATIONS

This section contains information on how to configure notification settings on your computer.

#### IN THIS SECTION:

About notification settings	<u>58</u>
Configuring notification settings	<u>58</u>
Disabling notifications	59

## **ABOUT NOTIFICATION SETTINGS**

Various events may occur when Kaspersky Rescue Disk runs. These might be of an advisory nature or contain important information. For example, an event can inform you that the application update was successfully completed, or can record an error that should be eliminated immediately.

When operating, Kaspersky Rescue Disk sends the following types of notifications:

- Critical notifications notifications about critically important events that point to problems with the Kaspersky
  Rescue Disk operation, or vulnerabilities in your computer's protection: for example, the application databases
  are corrupted, or the key has expired.
- Functional failures notifications about events which make the application inoperable: for example, no key or application databases.
- Important notifications notifications about important events that must be attended to, since they reflect important situations in the operation of Kaspersky Rescue Disk: for example, protection is disabled, or a full virus scan has not been performed for a long time.
- **Minor notifications** reference-type messages about events which as a rule do not contain important information: for example, all dangerous objects have been disinfected.

To enable / disable event notifications, click the **Settings** button, located in the top part of the main application window, select the **Notifications** section and check the **Enable events notifications** box.

In order to receive updates on Kaspersky Rescue Disk's operation, you can use the notification feature. By default, the user is notified with pop-up messages appearing for all events. You can also disable the notification displaying option (see section "Disabling notifications" on page <u>59</u>) and determine the type of notifications that you want to receive.

## SEE ALSO:

## **CONFIGURING NOTIFICATION SETTINGS**

- To configure notification settings:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. In the left part of the window select the **Notifications** section.
  - 3. Click the **Settings** button in the right part of the window.
  - 4. In the **Notifications** window that opens, check the boxes for those events about which you wish to receive notifications.

## **SEE ALSO:**

## **DISABLING NOTIFICATIONS**

- ➡ To disable notification delivery:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. In the left part of the window select the **Notifications** section.
  - 3. In the right part of the window, uncheck the **Enable events notifications** box.

Even if the notification display is disabled, information about events occurring during the application's operation will still be recorded in Kaspersky Rescue Disk's operation report.

## **SEE ALSO:**

## **REPORTS AND STORAGES**

This section groups the information about the parameters that regulate the work with report files and Kaspersky Rescue Disk repositories.

## IN THIS SECTION:

About configuring reports and storages	<u>60</u>
Logging non-critical events in a report	61
Storing reports	
Clearing the application reports	
Storing Quarantine and Backup objects	62

## ABOUT CONFIGURING REPORTS AND STORAGES

This section groups the information about the parameters that regulate work with Kaspersky Rescue Disk data files.

Application data files are objects that have been quarantined (see section "About Quarantine" on page  $\underline{32}$ ) or moved to the Backup (see section "About Backup" on page  $\underline{33}$ ), and reports (see section "About reports" on page  $\underline{35}$ ) about task execution.

In the **Reports and Storages** section of the Kaspersky Rescue Disk's settings window, you can perform the following actions:

- Log records into the report (see section "Logging non-critical events in a report" on page 61).
  - You can add records about non-critical events to the protection report. By default, these events are not added to the report.
- Modify report storage settings (see section "Storing reports" on page 61).
  - You can define the maximum storage time for the reports and define the maximum size of a report file. You can also cancel any limits set on the report's size, or enter another value.
- Delete information from reports (see section "Clearing the application reports" on page 61).
  - Information about the Kaspersky Rescue Disk operation is logged in the reports. You can clear them.
- Modify storage settings for quarantined and backup objects (see section "Storing Quarantine and Backup objects" on page 62).

You can determine the maximum storage time for quarantined objects and for copies of objects in the backup (the **Store objects no longer than** box). By default, the objects are stored for 30 days: after that, they will be deleted. You can change the maximum storage term or remove this restriction altogether. You can also specify the maximum size of data storage area (the **Maximum size** box). The default maximum size is 100 MB. You can cancel the report size limit or set another value for it.

## SEE ALSO:

eports35
----------

## LOGGING NON-CRITICAL EVENTS IN A REPORT

- ➡ To record non-critical events in a report:
  - 1. Open the main application window.
  - 2. Click the **Settings** link in the top part of the window. In the left part of the window select the **Reports and Storages** section.
  - 3. In the right part of the window, in the **Reports** section, check the **Log non-critical events** box.

## SEE ALSO:

About configuring reports and storages ......60

## **STORING REPORTS**

- ➡ To configure the report storage settings:
  - 1. Open the main application window.
  - Click the Settings link in the top part of the window. In the left part of the window select the Reports and Storages section.
  - 3. In the right part of the window in the **Reports** section specify:
    - Maximum storage time for event reports (the ✓ Store reports no longer than box). By default, it is equal
      to 30 days: after it expires, objects will be deleted. You can change the maximum storage time, or even
      discard any limits imposed on it.
    - Maximum size of report file (the **Maximum file size** box). By default, the maximum size is 1024 MB. Once the maximum size has been reached, the content of the file will be overwritten with new records. You can cancel any limits set on report size, or enter another value.

## SEE ALSO:

## **CLEARING THE APPLICATION REPORTS**

- To clear application reports:
  - 1. Open the main application window.
  - Click the Settings link in the top part of the window. In the left part of the window select the Reports and Storages section.

- 3. In the right part of the window, in the **Reports** section click the **Clear** button.
- 4. In the Clearing reports window, check the boxes for the report categories you want to clear.

#### **SEE ALSO:**

About configuring reports and storages	60

## STORING QUARANTINE AND BACKUP OBJECTS

- To configure the settings for storing Quarantine and Backup objects:
  - 1. Open the main application window.
  - Click the Settings link in the top part of the window. In the left part of the window select the Reports and Storages section.
  - 3. In the right part of the window, in the **Quarantine and Backup** section check the following boxes:
    - Store objects no longer than specifies the maximum storage time for objects in Quarantine and Backup.
    - Maximum size specifies the maximum size of data storage area.

After the specified period expires, or when the storage is full, the objects first placed in Quarantine or Backup will be deleted.

## **SEE ALSO:**

Quarantine and Backup	<u>32</u>
About configuring reports and storages	60

## **CLOSING KASPERSKY RESCUE DISK**

- To exit Kaspersky Rescue Disk:
  - 1. Click the icon \_\_\_\_\_, located in the left corner of the screen in the taskbar. A system menu will open.
  - 2. In the menu that opens, select the **Shut down the computer** item.
    - A dialog window with the following message appears: Do you really want to shut down the computer?
  - 3. Click the Yes button.

## WORKING WITH KASPERSKY RESCUE DISK IN TEXT MODE

This section describes Kaspersky Rescue Disk operating mode in text mode.

#### IN THIS SECTION:

About text mode	<u>63</u>
Working with file manager	<u>63</u>
Working with command prompt	<u>66</u>

## ABOUT TEXT MODE

Text mode represents a user interface that uses only alphanumeric characters and character graphics for input-output and information representation. Text mode uses few input-output devices resources (particularly memory) and high speed information displaying.

The Kaspersky Rescue Disk text mode combines the command prompt interface and the console mode offered by Midnight Commander file manager.

The following features are available in text mode:

- network configuration (network adapter, proxy server);
- starting the Kaspersky Rescue Disk console;
- · objects scan (autorun objects, boot sectors, disks, disk directories, all objects);
- update databases;
- · rolling back the last update;
- · help on command syntax;
- · restart computer;
- closing Kaspersky Rescue Disk on computer shutdown.

In text mode you can only start object scans and updates. To modify task settings, launch the application in the graphic mode (see section "Working with Kaspersky Rescue Disk in graphic mode" on page 18).

## **WORKING WITH FILE MANAGER**

This section describes the features of Kaspersky Rescue Disk file manager in text mode.

### IN THIS SECTION:

Network configuration	<u>6</u> 4
Starting the Kaspersky Rescue Disk console	<u>64</u>
Virus scan	<u>65</u>
Kaspersky Rescue Disk update	<u>65</u>
Rolling back to the previous databases	<u>65</u>
Viewing Help	<u>65</u>
Closing Kaspersky Rescue Disk	65

## **NETWORK SETUP**

- To configure a network adapter and change proxy server settings:
  - 1. In the user menu select **Network setup**. As a result, a **Network setup** window opens.
  - 2. In the window that opens, select one of the following options:
    - **Configure network adapter** to configure the network adapter.

Select a network adapter the settings of which you would like to modify. Click the **OK** button. As a result, a configuration window for the selected adapter opens. To modify its settings, click the **Yes** button. In the window that opens, select one of the following options:

- DHCP to configure the network adapter automatically.
- **Manual configuration** to specify the network adapter settings manually. Click the **OK** button. In the window that opens, specify the network adapter settings.

After configuring the network adapter settings, click the  ${\bf OK}$  button.

• Configure proxy server settings – to specify proxy server settings.

Click the **OK** button. In the window that opens, specify the proxy server settings. Click the **OK** button.

## STARTING THE KASPERSKY RESCUE DISK CONSOLE

To start the Kaspersky Rescue Disk console,

in the user menu, select the corresponding item.

## VIRUS SCAN

To start an objects scan task,

in the user menu select one of the following options:

Scan <Disk> – Kaspersky Rescue Disk scans each disk object (file) for viruses. If an infected or suspicious
object is found, the user is invited to take actions on it.

After treating the infected / suspicious object, Kaspersky Rescue Disk removes all hyperlinks to this object from the registry and Windows service directory files.

- Scan all objects Kaspersky Rescue Disk scans all files in all drives, including the autorun objects and boot sectors.
- Scan startup object Kaspersky Rescue Disk scans the registry and files with .inf, .ini, .bat extensions of Windows service directories on all connected drives. Each object is scanned for viruses. If an infected or suspicious object is found, the user is invited to take actions on it.

After treating the infected / suspicious object, Kaspersky Rescue Disk removes all hyperlinks to this object from the registry and Windows service directory files.

• Scan disk boot sectors – Kaspersky Rescue Disk scans each disk boot sector for malicious objects. If a malicious object is found, the user can select an action on such object.

After treating the malicious object, Kaspersky Rescue Disk removes all hyperlinks to this object from the registry and Windows service directory files.

## KASPERSKY RESCUE DISK UPDATE

To start the update task,

in the user menu, select Start update.

## **ROLLING BACK TO THE PREVIOUS DATABASES**

To roll back to the previous databases,

in the user menu, select the corresponding item.

## VIEWING HELP

To view the help for the key combinations in the file manager,

in the user menu, select Help.

## CLOSING KASPERSKY RESCUE DISK

To exit Kaspersky Rescue Disk,

in the user menu or command catalog, select Shut down the computer / Restart computer.

## **WORKING WITH COMMAND PROMPT**

This section describes how to work with Kaspersky Rescue Disk in text mode.

## IN THIS SECTION:

Command prompt syntax	<u>66</u>
Virus scan	
Kaspersky Rescue Disk update	<u>68</u>
Rolling back the last update	<u>69</u>
Viewing Help	<u>69</u>
Closing Kaspersky Rescue Disk	69

## **COMMAND PROMPT SYNTAX**

## Command prompt syntax:

<command> [settings]

The following may be used as commands:

HELP	help on command syntax, displaying the list of commands
SCAN	Scans objects for viruses
UPDATE	Launches update task
ROLLBACK	Rolls back the most recent update
EXIT	Closing Kaspersky Rescue Disk

## **VIRUS SCAN**

Starting a scan of a certain area for viruses and processing malicious objects from the command prompt generally looks as follows:

SCAN [<scan object>] [<action>] [<file types>] [<exclusions>] [<report settings>]

Disk names must be specified in upper-case, for example C:/file.txt, where C - is the disk name.

## Settings description:

Octamigo docempnom.		
<object scanned=""> – this setting gives the list of objects that will be scanned for malicious code.</object>		
The setting can include several values fr	rom the list provided, separated by spaces.	
<files></files>	List of paths to the files and/or folders to be scanned.	
	You can enter an absolute or relative path to the file. Items on the list are separated by a space.	
	Notes:	
	If the object name contains a space, it must be placed in quotation marks.	
	If you specify a concrete folder, all the files in it are scanned.	
<disc_name>:/<folder></folder></disc_name>	Scan the specified disk where <disc_name> is the name of the disk, and <folder> is the path to the folder to be scanned.</folder></disc_name>	
<action> - this setting determines what setting has not been defined, the default</action>	action will be taken with malicious objects detected during the scan. If this action is the one with the value for <b>-i8</b> .	
-i0	Take no action on the object; simply record information about it in the report.	
-i1	Treat infected objects and if disinfection is impossible, skip.	
-i2	Treat infected objects and if disinfection fails, delete. Do not delete infected objects from compound objects. Delete infected compound objects with executable headers (.sfx archives).	
-i3	Treat infected objects and if disinfection fails, delete. Delete all compound objects completely if infected parts cannot be deleted.	
-i4	Delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.	
-i8	Prompt the user for action if an infected object is detected.	
-i9	Prompt the user for action at the end of the scan.	

<b><file types=""> -</file></b> this setting defines the file types that will be subject to an anti-virus scan. If this setting is not defined, by default infected files are only scanned by content.		
-fe	Scan only infected files by extension.	
-fi	Scan only infected files by contents.	
-fa	Scan all files.	
<exclusions> - this setting defines objects that are excluded from the scan.</exclusions>		
The setting can include several values from the list provided, separated by spaces.		
-e:a	Do not scan archives.	
-e:b	Do not scan email databases.	
-e:m	Do not scan plain text emails.	
-e: <filemask></filemask>	Do not scan objects by mask.	
-e: <seconds></seconds>	Skip objects that are scanned for longer than the time specified in the <seconds> setting.</seconds>	
-es: <container limit="" size=""></container>	Skip compound files which size (in MB) exceeds the value specified by the <b><container limit="" size=""></container></b> parameter.	

## Example:

Run the scan of the Documents and Settings folder and the <D> disk:

SCAN D: "C:/Documents and Settings"

## KASPERSKY RESCUE DISK UPDATE

The syntax for updating the databases and modules of Kaspersky Rescue Disk from the command line is as follows:

UPDATE [<update\_source>] [-R[A]:<report\_file>]

Disk names must be specified in upper-case, for example C:/file.txt, where C - is the disk name.

## Settings description:

<update_source></update_source>	The name of a HTTP or FTP server or network folder for downloading updates. The value for the parameter may be in the form of a full path to an update source or a URL. If a path is not selected, the update source will be taken from the update settings.
-R[A]: <report_file></report_file>	-R: <report_file> - log only important events in the report.</report_file>
	-RA: <report_file> – log all events in the report.</report_file>
	You can use an absolute path to the file. If the setting is not defined, the scan results are displayed on screen and all events are displayed.

## Example:

Update databases and record all events in a report:

UPDATE -RA:C:/avbases upd.txt

## **ROLLING BACK THE LAST UPDATE**

## Command syntax:

ROLLBACK [-R[A]:<report file>]

Disk names must be specified in upper-case, for example C:/file.txt, where C - is the disk name.

## Settings description:

-R[A]: <report_file></report_file>	-R: <report_file> - log only important events in the report.</report_file>
	-RA: <report_file> - log all events in the report.</report_file>
	You can use an absolute path to the file. If the setting is not defined, the scan results are displayed on screen and all events are displayed.

## Example:

Roll back report:

ROLLBACK -RA:C:/rollback.txt

## VIEWING HELP

Use this command to view the help on application command line syntax:

HELP

To get help on the syntax of a specific command, you can use one of the following commands:

<command> -?
HELP <command>

## **CLOSING KASPERSKY RESCUE DISK**

To close Kaspersky Rescue Disk, enter the following command in the command prompt:

exit

## HARDWARE INFORMATION

The **Hardware information** task should be used if Kaspersky Rescue Disk could not be started either in graphic or text mode because the hardware is not supported.

The **Hardware information** task gives you the possibility of storing information on computer hardware in electronic form. Before starting the task, install a removable drive to which all the hardware information will be saved.

The hardware information cannot be saved using the CD / DVD-RW removable drive.

After the task is completed, you can save information, restart or shut down the computer, by selecting the corresponding option in the dialog window that opens. To switch between options, press the **TAB** key. To confirm the selection, press the **ENTER** key.

After this function is completed, save the information to your removable drive and send this information to the Technical Support Service (see section "Contacting the Technical Support Service" on page 72) specialists.

If you do not have a removable drive, you can write information manually or print a screen with the specified data.

# RESTRICTIONS IN THE APPLICATION OPERATION

The application currently has the following limitations:

- If the graphic mode is selected, the computer shuts down and Kaspersky Rescue Disk is not loaded. The most common problem that may be encountered when loading the graphic subsystem is that the driver of a video adapter or output device cannot be detected.
- Kaspersky Rescue Disk does not display logical drives when selecting the scan area, only boot sectors are
  displayed. The most likely problem that may be encountered is that file systems on hard drives and USB
  devices that had been connected, have not been detected probably due to the use of RAID.

# CONTACTING THE TECHNICAL SUPPORT SERVICE

If problems occur during Kaspersky Rescue Disk operation, first of all check if the method for solving them is described in the documentation, help, Knowledge Base on the Kaspersky Lab Technical Support website, or on the User Forum.

If you cannot find a solution to your problem, please contact Kaspersky Lab Technical Support Service in one of the following ways:

- send a query from the Personal Cabinet at the Technical Support Service website;
- make a phone call.

Technical Support Service specialists will answer any of your questions about installing, activating and using the application. If your computer has been infected, they will help you remove the consequences of malware activity.

Before contacting the Technical Support Service please read the support rules.

When you contact the Technical Support Service, service specialists may ask you to compile a trace file and send it to the Technical Support Service.

#### IN THIS SECTION:

My Kaspersky Account	<u>72</u>
Technical support by phone	<u>73</u>
Creating and saving the trace file	<u>73</u>

## MY KASPERSKY ACCOUNT

My Kaspersky account – is your personal section at the Technical Support website. You may perform the following actions in My Kaspersky Account:

- contact Technical Support Service and Virus Lab;
- contact the Technical Support Service without using the email;
- track your requests' status in real time;
- view a detailed history of your requests to the Technical Support Service.

To log into the My Kaspersky Account, in the address bar of your browser, type https://my.kaspersky.com.

If you do not have an account yet, you can register at the My Kaspersky Account registration page. Enter your email address and a password to log in My Kaspersky Account.

Note that some requests should not be addressed to the Technical Support Service, but to the Kaspersky Virus Lab. These are requests of the following types:

- unknown malicious program you suspect that an object is malicious, while Kaspersky Rescue Disk does not classify it as such;
- false alarm Kaspersky Rescue Disk classifies a file as a virus, yet you are sure that the file is healthy;
- description of the malicious program you want to get a description of a specified virus.

You do not need to be a registered user of My Kaspersky Account to be able to send requests to Kaspersky Virus Lab from the page with request form.

You can find the details on the page of questions and answers about My Kaspersky Account, at the Technical Support Service website.

## **TECHNICAL SUPPORT BY PHONE**

If you have an urgent problem you can call your local Technical Support Service. Before calling Russian-speaking or international technical support specialists, please collect the information about your computer and the anti-virus application on it. This will enable our specialists to help you more quickly.

## **CREATING AND SAVING THE TRACE FILE**

If there are failures in the Kaspersky Rescue Disk operation, the Technical Support Service can ask you to create a trace file.

- To create and save the trace file:
  - In the start up wizard window, select the graphic interface language using the cursor moving keys. Click the ENTER button.

A window with various options will open.

- 2. Select the loading mode that you need.
- 3. Press the **E** key.
- 4. At the end of the first line after quiet following a space insert trace.
- Press the CTRL+X keyboard shortcut.

The trace file will be saved.

When working with Kaspersky Rescue Disk, you can get access the file using the task manager. The file will be located under the following path: /discs/<Hard disk>:/Kaspersky Rescue Disk/avp<unique combination of date, time and internal data>.log.

After closing Kaspersky Rescue Disk, the file will be archived and located under the following path: **<Hard** drive>:/Kaspersky Rescue Disk/kavrescue\_sysinfo\_<file creation date>.

## **GLOSSARY**

## A

#### **APPLICATION SETTINGS**

Application settings which are common for all task types, regulating the application's operation as a whole, such as application performance settings, report settings, backup storage settings.

## В

#### **BACKUP STORAGE**

Special storage designed to save backup copies of objects created before their first disinfection or deletion.

## D

#### **DATABASE UPDATES**

One of the functions performed by a Kaspersky Lab application that enables it to keep protection current. In this case, the databases are downloaded from the Kaspersky Lab update servers onto the computer and are automatically connected to the application.

#### **D**ATABASES

Databases created by Kaspersky Lab's experts and containing detailed description of all currently existing threats to computer security as well as methods used for their detection and disinfection. Kaspersky Lab constantly updates the databases as new threats appear. In order to achieve higher quality of threat detection we recommend that you copy databases from Kaspersky Lab's update servers on a regular basis.

## **DELETING AN OBJECT**

The method of processing objects which ends in it being physically deleted from its original location (hard drive, folder, network resource). We recommend that this method be applied to dangerous objects which, for any reason, cannot be disinfected.

### **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. Kaspersky Lab allows scanning boot sectors for viruses and disinfecting them if an infection is found.

## Ε

## **EXCLUSION**

Exclusion is an object excluded from the scan by Kaspersky Lab application. You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects by threat type according the Virus Encyclopedia classification. Each task can be assigned a set of exclusions.

## Н

## **HEURISTIC ANALYZER**

Threat detection technology for threats that cannot be detected using Anti-Virus databases. It allows detecting objects suspected of being infected with an unknown virus or a new modification of the known viruses.

Heuristic analyzer helps to detect up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

#### INFECTED OBJECT

Object containing malicious code. It is detected when a section of the object's code completely matches a section of the code of a known threat. Kaspersky Lab does not recommend using such objects since they may infect your computer.

K

## KASPERSKY LAB'S UPDATE SERVERS

A list of Kaspersky Lab's HTTP and FTP servers from which the application downloads databases and module updates to your computer.

M

## MOVING OBJECTS TO QUARANTINE

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection.

0

## **OBJECT DISINFECTION**

The method used for processing infected objects that results in complete or partial recovery of data, or the decision that the objects cannot be disinfected. Objects are disinfected using the database records. If disinfection is the primary action to be performed with the object (that is, the first action to be performed with the object immediately it is detected) a backup copy of the object will be created before disinfection is attempted. Part of the data may be lost during disinfection. This backup copy can be used to restore the object to its original state.

P

## POTENTIALLY INFECTED OBJECT

An object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected using heuristic analyzer.

#### **PROTECTION STATUS**

The current status of protection, summarizing the degree of security of the computer.

#### **PROXY SERVER**

Computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then, the proxy server either connects to the specified server and obtains the resource from it, or returns the resource from its own cache (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 specific purposes.

## Q

## QUARANTINE

A certain folder into which all possibly infected objects are placed, which were detected during scans or by real-time protection.

## R

## RECOMMENDED LEVEL

Level of security based on application settings recommended by Kaspersky Lab experts to provide the optimal level of protection for your computer. This level is set to be used by default.

## RESTORATION

Moving an original object from Quarantine or Backup to the folder where it was originally found before being moved to Quarantine, disinfected, or deleted, or to a different folder specified by the user.

## U

## UPDATE

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

## **KASPERSKY LAB ZAO**

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

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

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

Our company's most valuable assets are the unique knowledge and expertise accumulated by its specialists during fourteen years fighting continuously against computer viruses. A thorough analysis of computer virus activities enables the company's specialists to foresee trends in malware development, and deliver to our users timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. At all times, the company's products remain one step ahead of other vendors in delivering anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its convenient and easy-to-use management tools maximize the degree of automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

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

If you have any questions, you can contact our dealers or contact Kaspersky Lab directly. We will be glad to assist you, via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.viruslist.com
Virus Lab:	newvirus@kaspersky.com
	(only for sending suspicious objects in archives)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en
	(for virus analysts' queries)
Kaspersky Lab web forum:	http://forum.kaspersky.com

## **INFORMATION ON THIRD-PARTY CODE**

When creating the application, the third-party code was used.

#### IN THIS SECTION:

Program code	<u>78</u>
Developer tools	<u>78</u>
Distributable program code	<u>78</u>
Other information	<u>78</u>

## **PROGRAM CODE**

Information on the third-party code used when creating an application, is collected in the rescue/help/License notice 1.txt file.

## **DEVELOPER TOOLS**

Information on developer tools and other third-party means used when creating an application, is collected in the /rescue/help/License\_notice\_2.txt file.

## **DISTRIBUTABLE PROGRAM CODE**

The application includes the independent binary third-party program code. The license texts of a program code, distributed on the conditions of GNU GPL and GNU LGPL licenses, are collected in the /rescue/help/License notice 3.txt file.

## **OTHER INFORMATION**

"Agava-C" program library, developed by OOO "R-Alpha", is used to check digital signature.

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to <a href="mailto:source@kaspersky.com">source@kaspersky.com</a> or the source code is supplied with the Software.

Additional information on the third-party code is collected in the /rescue/help/License\_notice\_4.txt file.

## **INDEX**

^	
Actions on objects	47
Application installation	
Application interface	18, 20
В	
Backup storage	32, 34, 62
Browser configuration	24
D	
Detectable threat categories	52
Disk image	
E	
Excluding from scan	29
G	
Grouping information	37
н	
Hardware requirements	1
I .	
Installation	
applicationdisk image	
K	
Kaspersky Lab	77
M	
Main application features	1 <sup>,</sup>
Main application window	20
Maximum size object to be scanned	48
Quarantine	
N	
Network	
proxy server	
Notifications configuring the settings	
disabling	
0	
Object type	47
P	
Preparing to load	

Protection icon	25
Protection status	25
Proxy server	24, 64
Q	
Quarantine	
deleting an object	
restoring an object	
viewing objects	
Quarantine and Backup	32
R	
Reports	
event type	
events search	
filtering	
saving to file	
selecting a component or a task	
viewing	
Rescue disk	
	00
S	
Scan	47
action on detected object	
pausing a taskscan of compound files	
security level	
tasks	
type of objects to be scanned	
Scan method	
Security level scan	
Software requirements	
Starting a task	-
SCAN	28
update	
Statistics	43
Storages	
Backup storage	
Quarantine	32, 34
Т	
Taskbar	
Threat types	
Threats	
Toolbar	
Trusted zone	
exclusion rules	54, 55, 56
U	
Update	
regional settings	53
rolling back the last update	
update source	
update task	30, 51, 68
Update source	52, 53

Updating the application......30, 51