

Kaspersky Anti-Virus 6.0 for Windows Servers MP4

USER GUIDE

APPLICATION VERSION: 6.0 MAINTENANCE PACK 4, CRITICAL FIX 1



KASPERSKY lab

Dear User of Kaspersky Anti-Virus!

Thank you for choosing our product. We hope that this documentation helps you in your work and provides answers you may need.

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

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 notification. For the latest version of this document please refer to Kaspersky Lab's website at <http://www.kaspersky.com/docs>.

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: 25.02.2010

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

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

TABLE OF CONTENTS

INTRODUCTION	8
Distribution Kit.....	8
End user license agreement (EULA)	8
Services provided for registered users.....	8
Hardware and software system requirements.....	9
KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	10
Obtaining information about the application.....	10
Sources of information to research on your own	10
Contacting the Sales Department	11
Contacting the Technical Support service	11
Discussing Kaspersky Lab's applications on the web forum	12
What's new in Kaspersky Anti-Virus 6.0 for Windows Servers MP4	12
What Kaspersky Anti-Virus defense is built on	13
File Anti-Virus.....	13
Virus scan tasks	14
Update.....	14
Support features of the application.....	14
INSTALLING KASPERSKY ANTI-VIRUS 6.0.....	16
Installation using the Installation Wizard.....	16
Step 1. Verifying that the system meets the installation requirements	17
Step 2. Installation start window.....	17
Step 3. Viewing the License Agreement	17
Step 4. Selecting installation folder	17
Step 5. Using application settings saved after previous installation	17
Step 6. Selecting the type of the installation.....	18
Step 7. Selecting application components for the installation.....	18
Step 9. Searching for other anti-virus applications	18
Step 10. Final preparation for installation	19
Step 11. Completing the installation.....	19
Application installation from the command line	19
Installation from Group Policy Object editor.....	20
Installing the application	20
Description of setup.ini file settings	20
Updating application version	21
Removing the application	21
GETTING STARTED.....	22
Initial Configuration Wizard	22
Using the objects saved from the previous version	23
Activating the application.....	23
Update settings configuration.....	25
Configuring virus scan schedule	25
Restricting access to the application	25
Finishing the Configuration Wizard	26
Scanning computer for viruses	26

- Updating the application 26
- Managing licenses 27
- Security management 28
- Pausing protection 29
- Eliminating problems. User technical support 29
- Creating a trace file 29
- Configuring application settings 30
- Application operation reports. Data files 30
- APPLICATION INTERFACE 31**
 - Taskbar notification area icon 31
 - Context menu 32
 - Main application window 33
 - Notifications 34
 - Application settings window 35
- FILE ANTI-VIRUS..... 36**
 - Component operation algorithm 37
 - Changing security level 38
 - Changing actions to be performed on detected objects 38
 - Creating a protection scope 39
 - Using heuristic analysis 40
 - Scan optimization 41
 - Scan of compound files 41
 - Scanning large compound files 41
 - Changing the scan mode 42
 - Scan technology 42
 - Pausing the component: creating a schedule 43
 - Pausing the component: creating a list of applications 43
 - Restoring default protection settings 43
 - File Anti-Virus statistics 44
 - Delayed object treatment 44
- SERVER VIRUS SCAN 46**
 - Starting the virus scan 47
 - Creating a list of objects to scan 48
 - Changing security level 49
 - Changing actions to be performed on detected objects 49
 - Changing the type of objects to scan 50
 - Scan optimization 51
 - Scan of compound files 52
 - Changing the scan method 52
 - Scan technology 52
 - Computer performance during task execution 53
 - Pausing the task: creating a schedule 53
 - Pausing the component: creating a list of applications 54
 - Run mode: specifying an account 54
 - Run mode: creating a schedule 55
 - Features of scheduled task launch 55
 - Virus scan statistics 56
 - Assigning common scan settings for all tasks 56

Restoring default scan settings	56
UPDATING THE APPLICATION	58
Starting the update	59
Rolling back the last update	60
Selecting an update source	60
Regional settings	61
Using a proxy server	61
Run mode: specifying an account	61
Run mode: creating a schedule	62
Selecting objects to update	62
Changing the update task's run mode	63
Updating from a local folder	63
Update statistics	64
Possible problems during the update	64
CONFIGURING APPLICATION SETTINGS	69
Protection	70
Enabling / disabling computer protection	71
Launching the application at the operating system startup	71
Selecting detectable threat categories	71
Creating a trusted zone	72
Exporting / importing Kaspersky Anti-Virus settings	75
Restoring the default settings	76
File Anti-Virus	76
Scan	77
Update	78
Options	78
Application self-defense	78
Application access restriction	79
Restricting the size of iSwift files	80
Multiprocessor server configuration	80
Notifications about Kaspersky Anti-Virus events	81
Active interface elements	82
Reports and Storages	83
Principles of handling reports	84
Configuring reports	84
Quarantine for potentially infected objects	85
Actions on quarantined objects	85
Backup copies of dangerous objects	86
Working with backup copies	86
Configuring quarantine and backup	86
RESCUE DISK	87
Creating the Rescue Disk	88
Step 1. Selecting the disk image source	88
Step 2. Copying ISO image	88
Step 3. ISO image update	88
Step 4. Remote startup	89
Step 5. Closing the Wizard	89
Booting the computer using the Rescue Disk	89

Working with Kaspersky Rescue Disk from the command prompt.....	91
Virus scan	91
Kaspersky Anti-Virus update	93
Rolling back the last update	93
Viewing Help	93
VALIDATING KASPERSKY ANTI-VIRUS SETTINGS	95
Test "virus" EICAR and its modifications	95
Validating File Anti-Virus settings	96
Validating virus scan task settings	97
TYPES OF NOTIFICATIONS	98
Malicious object detected.....	98
Object cannot be disinfected.....	99
Suspicious object detected	99
WORKING WITH THE APPLICATION FROM THE COMMAND LINE.....	101
Viewing Help.....	102
Virus scan.....	102
Updating the application	104
Rolling back the last update.....	105
Starting / stopping File Anti-Virus operation or a task.....	105
Statistics on a component's operation or a task.....	106
Exporting protection settings.....	107
Importing protection settings.....	107
Activating the application	107
Restoring a file from quarantine.....	108
Closing the application.....	108
Obtaining a trace file.....	108
Return codes of the command line	109
MODIFYING, REPAIRING, OR REMOVING THE APPLICATION.....	110
Modifying, repairing, and removing the application using the Installation Wizard	110
Step 1. Installation Welcome window	110
Step 2. Selecting an operation	110
Step 3. Completing application modification, repair, or removal.....	111
Removing the application from the command prompt.....	111
MANAGING THE APPLICATION VIA KASPERSKY ADMINISTRATION KIT.....	113
Managing the application.....	115
Starting and stopping the application	116
Configuring application settings	117
Configuring specific settings.....	118
Managing tasks.....	119
Starting and stopping tasks.....	121
Creating tasks	121
Local Task Wizard.....	122
Configuring tasks	123
Managing policies	125
Creating policies.....	125
Policy Creation Wizard.....	126
Configuring the policy.....	128

USING THIRD-PARTY CODE..... 130

 Boost-1.30.0 library..... 131

 LZMA SDK 4.40, 4.43 library 131

 Windows Template Library 7.5 131

 Windows Installer XML (WiX) toolset 2.0 library 132

 ZIP-2.31 library 135

 ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 library 136

 UNZIP-5.51 library 136

 LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 library 137

 LIBJPEG-6B library..... 139

 LIBUNGIF-4.1.4 library 141

 MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 library..... 141

 MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 library..... 141

 INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 library 141

 CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 library..... 142

 COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum library 142

 PLATFORM INDEPENDENT IMAGE CLASS library..... 142

 FLEX PARSER (FLEXLEXER)-V. 1993 library..... 143

 ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 library 143

 STDSTRING- V. 1999 library 144

 T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 library 144

 NTSERVICE- V. 1997 library 145

 SHA-1-1.2 library 145

 COCOA SAMPLE CODE- V. 18.07.2007 library..... 146

 PUTTY SOURCES-25.09.2008 library..... 146

 Other information 147

GLOSSARY..... 148

KASPERSKY LAB..... 154

LICENSE AGREEMENT 155

INDEX 160

INTRODUCTION

IN THIS SECTION

Distribution Kit	8
Services provided for registered users	8
Hardware and software system requirements	9

DISTRIBUTION KIT

You can purchase the boxed version of Kaspersky Anti-Virus from our resellers, or purchase it from online stores, such as the **eStore** section at <http://www.kaspersky.com>.

If you purchase the boxed version of the product, the package will include:

- Sealed envelope with the installation CD containing the program files and documentation in PDF format.
- User Guide in printed form (if this item has been included in the order), or Product Guide.
- Application key file attached to the installation CD envelope.
- Registration card (with serial number of the product).
- End user license agreement (EULA).

Before unsealing the installation CD envelope, carefully read through the EULA.

If you buy Kaspersky Anti-Virus from eStore, you will download the product from the Kaspersky Lab website; the present User Guide is included with the installation package. You will be sent a key file by email after your payment has been received.

END USER LICENSE AGREEMENT (EULA)

The End User License Agreement is a legal agreement between you and Kaspersky Lab that specifies the terms under which you may use the software you have purchased.

Read the EULA through carefully!

If you do not agree with the terms of the EULA, you can return your boxed product to the reseller from whom you purchased it, and be reimbursed the amount you paid for the application, provided that the envelope containing the installation disk is still sealed.

By opening the sealed envelope with the installation CD, you accept all the terms of the EULA.

SERVICES PROVIDED FOR REGISTERED USERS

Kaspersky Lab offers an extensive service package to all legally registered users, thus enabling them to boost the application's performance.

After purchasing a license, you become a registered user and, during the period of your license, you will be provided with the following services:

- hourly updates to the application databases and updates to the software package;
- support on issues related to the installation, configuration and use of the purchased software product. Services will be provided by phone or by email;
- notifications about new Kaspersky Lab products and new viruses appearing worldwide. This service is available to users who have subscribed to Kaspersky Lab news mailing at the Technical Support Service website (<http://support.kaspersky.com/subscribe/>).

Support on issues related to the performance and the use of operating systems, third-party software, or other technologies, is not provided.

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

For a proper functioning of Kaspersky Anti-Virus 6.0, the computer should meet these minimum requirements:

General requirements:

- 300 MB free hard drive space.
- Microsoft Internet Explorer 6.0, or higher (for updating application databases and program modules via the Internet).
- Microsoft Windows Installer 2.0, or higher.

Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:

- Intel Pentium 400 MHz 32-bit (x86) / 64-bit (x64) processor, or higher (or a compatible equivalent).
- 512 MB free RAM.

Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 or higher), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 or higher), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:

- Intel Pentium 1 GHz 32-bit (x86) / 1.4 GHz 64-bit (x64) processor, or higher (or a compatible equivalent).
- 1 GB free RAM.

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 is a new generation of data security products.

IN THIS SECTION

Obtaining information about the application	10
What's new in Kaspersky Anti-Virus 6.0 for Windows Servers MP4.....	12
What Kaspersky Anti-Virus defense is built on	13

OBTAINING INFORMATION ABOUT THE APPLICATION

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

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

IN THIS SECTION

Sources of information to research on your own	10
Contacting the Sales Department.....	11
Contacting the Technical Support service	11
Discussing Kaspersky Lab's applications on the web forum	12

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

http://www.kaspersky.com/anti-virus_windows_server

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

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

http://support.kaspersky.com/windows_file_server

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

These articles contain useful information, recommendations and FAQ on purchasing, installation and use of the application. They are assorted by their subject, such as Managing key files, Setting database updates, or Eliminating operation failures. The articles may provide answers to the questions that concern not only this application but the other Kaspersky Lab products as well; they may also contain the news from Technical Support service.

Help system

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

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

Documentation

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

CONTACTING THE SALES DEPARTMENT

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

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

The service languages are Russian and English.

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

CONTACTING THE TECHNICAL SUPPORT SERVICE

If you have already purchased Kaspersky Anti-Virus, you can obtain information about it from the Technical Support service, either over the phone or via the Internet.

Technical Support service specialists will answer any of your questions about installing and using the application. They will also help you eliminate the consequences of malware activities if your computer has been infected.

Before contacting the Technical Support Service, please read the Technical Support Terms and Conditions (<http://support.kaspersky.com/support/rules>).

An email request to the Technical Support Service

You can send your question to the Technical Support Service specialists by filling out the Helpdesk web form (<http://support.kaspersky.com/helpdesk.html>).

You can ask your question in Russian, English, German, French or Spanish.

In order to send an email request, you must indicate the **customer ID** obtained during the registration at the Technical Support Service website along with the **password**.

If you are not a registered user of Kaspersky Lab's applications yet, you can fill out a registration form at <https://support.kaspersky.com/en/personalcabinet/registration/form/>. When registering, you will have to enter the *activation code* or the *name of your license key file*.

The Technical Support Service will respond to your request in your Kaspersky Account (<https://support.kaspersky.com/en/PersonalCabinet>) and by the email you have specified in your request.

Describe the problem you have encountered in the request web form providing as much detail as possible. Specify the following in the mandatory fields:

- **Request type.** Select the subject that corresponds to the problem the most strictly, for example: Problem with product installation/uninstallation, or Problem with searching/eliminating viruses. If you have not found an appropriate topic, select "General Question".
- **Application name and version number.**
- **Request text.** Describe the problem you have encountered providing as much details as possible.
- **Customer ID and password.** Enter the client number and the password you have received during the registration at the Technical Support service website.
- **Email address.** The Technical Support service will send an answer to your question to this email address.

Technical support by phone

If you have an urgent problem you can call your local Technical Support service. Before contacting Russian-speaking (http://support.kaspersky.ru/support/support_local) or international (<http://support.kaspersky.com/support/international>) Technical Support specialists, please gather the information (<http://support.kaspersky.com/support/details>) about your computer and the anti-virus application installed on it. This will let our specialists help you more quickly.

DISCUSSING KASPERSKY LAB'S 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 <http://forum.kaspersky.com>.

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

WHAT'S NEW IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4

Kaspersky Anti-Virus 6.0 is a comprehensive data protection tool. Let us take a closer look at the innovations in Kaspersky Anti-Virus 6.0.

New in protection:

- The new antivirus kernel that Kaspersky Anti-Virus uses detects malicious programs more effectively. Additionally, the new antivirus kernel is significantly faster in scanning the system for viruses. This is the result of improved object processing and optimized use of computer resources (particularly for dual or quad core processors).
- A new heuristic analyzer has been implemented, providing more accurate detection and blocking of previously unknown malicious programs. If a program's signature has not been found in anti-virus databases, the heuristic analyzer simulates the launch of the program in an isolated virtual environment. This method is secure and allows for analyzing all of the effects of a program before it runs in a real environment.
- The update procedure for the application has been improved. The computer now rarely needs to be restarted.

New interface features:

- The interface makes the features of the program simple and easy to access.
- The interface has been redesigned with regard to the needs of administrators of small to midsized networks as well as administrators of large corporate networks.

New features in Kaspersky Administration Kit:

- Kaspersky Administration Kit makes management of a company's antivirus protection systems easy and simple. Administrators can use the application to manage protection of a corporate network of any size centrally, with tens of thousands of nodes, including remote and mobile users.
- A feature has been added that enables remote installation of the application with the latest version of the application databases.
- Management of the application when installed on a remote computer has been improved (policy structure has been redesigned).
- A feature has been added that allows to use an existing application configuration file when creating a policy.
- Another important feature is realized in option of creating specific configurations for mobile users when configuring group update tasks.
- One more feature has been implemented that allows to disable temporarily policy actions and group tasks for client computers with the application installed (after entering the correct password).

WHAT KASPERSKY ANTI-VIRUS DEFENSE IS BUILT ON

Kaspersky Anti-Virus for Windows Servers protection includes:

- File Anti-Virus (see page [13](#)) which monitors the computer's file system in real-time mode.
- Virus scan tasks (on page [14](#)), which are used to scan the entire computer or separate files, folders, drives and areas for viruses.
- Update (see page [14](#)) ensuring the up-to-date status of the internal application modules, and the databases used to scan for malicious programs.
- Support features (see section "Application support features" on page [14](#)) provide information support for working with the application and expanding its capabilities.

FILE ANTI-VIRUS

The server is protected in real-time using File Anti-Virus.

A file system can contain viruses and other dangerous programs. Malicious programs can be stored in your file system for years after one day making it through on a removable drive or from the Internet without showing themselves at all. But you need only open the infected file, and the virus is instantly activated.

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

VIRUS SCAN TASKS

In addition to File Anti-Virus's protection, it is extremely important to scan the server for viruses occasionally. This is necessary to rule out the possibility of spreading malicious programs that have not been discovered by File Anti-Virus, for example, because the security level is set at low or for other reasons.

The following virus scan tasks are included in Kaspersky Anti-Virus:

Scan

Scan of objects selected by the user. You can scan any object in the computer's file system.

Full Scan

A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded at startup, system backup, email databases, hard drives, removable storage media, and network drives.

Quick Scan

Virus scan of operating system startup objects.

UPDATE

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

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

SUPPORT FEATURES OF THE APPLICATION

Kaspersky Anti-Virus includes a number of support features. They are designed to keep the application up-to-date, to expand its capabilities, and to assist you in using the application.

Data files

When using the application, each protection component, virus scan task and application update creates a report. It contains the information about performed activities and the results; with them, you will be able to learn the details of how any Kaspersky Anti-Virus component works. Should problems arise, you can send the reports to Kaspersky Lab so that our specialists can study the situation in greater depth and help you as quickly as possible.

Kaspersky Anti-Virus moves all files suspected of being dangerous, to the special storage area called *Quarantine*. They are stored there in an encrypted form as to avoid infecting the computer. You can scan these objects for viruses, restore them to their previous locations, delete them, or place files to quarantine on your own. All files that turn out to be not infected upon completion of the virus scan, are automatically restored to their former locations.

The *Backup* holds copies of files disinfected and deleted by Kaspersky Anti-Virus. These copies are created so that you can restore the files or a picture of their infection, if necessary. The backup copies of the files are also stored in an encrypted form to avoid further infections.

You can restore a file from the backup copy to the original location and delete the copy.

Rescue Disk

Rescue Disk is designed to scan and disinfect infected x86-compatible computers. It should be used when the infection is at such level that it is deemed impossible to disinfect the computer using anti-virus applications or malware removal utilities.

License

When you purchase Kaspersky Anti-Virus, you enter into a license agreement with Kaspersky Lab which governs the use of the application, and your access to application database updates and Technical Support for a specified period of time. The term of use and other information required for the application's full functionality are provided in the license.

Using the **License** function, you can obtain detailed information about your current license, purchase a new license, or renew the existing one.

Support

All registered Kaspersky Anti-Virus users can take advantage of our Technical Support Service. To see the information about where to obtain technical support, use the **Support** function.

Using the links provided, you can go to the Kaspersky Lab product user forum and browse a list of frequently asked questions that might provide a solution to your problem. Additionally, you can fill out the special form on the site and send Technical Support a message regarding an error or a comment on program operation.

You also have access to the online Technical Support Service, and, of course, our personnel are always ready to provide you with telephone support about Kaspersky Anti-Virus.

INSTALLING KASPERSKY ANTI-VIRUS 6.0

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 can be installed on a computer in several ways:

- local installation – application installation on a single computer. Direct access to that computer is required for the installation to run and complete. Local installation can be carried out in one of the following modes:
 - interactive mode, using the application installation wizard (see section "Installation using the Installation Wizard" on page [16](#)); this mode requires the participation from the user when installing;
 - non-interactive mode in which the application installation is launched from the command line and does not require the participation from the user when installing (see section "Application installation from command line" on page [19](#)).
- remote installation – application installation on networked computers managed remotely from an administrator's workstation using the following:
 - Kaspersky Administration Kit software set (see Kaspersky Administration Kit Deployment Guide);
 - group domain policies of Microsoft Windows Server 2000/2003 (see section "Installation from Group Policy Object editor" on page [20](#)).

Before Kaspersky Anti-Virus installation begins (including remote one), it is recommended to close all active applications.

IN THIS SECTION

Installation using the Installation Wizard.....	16
Application installation from the command line.....	19
Installation from Group Policy Object editor	20

INSTALLATION USING THE INSTALLATION WIZARD

To install Kaspersky Anti-Virus on your computer, run the installation file on the product CD.

Installing the application from the installation file downloaded via the Internet, is identical to installing the application from the CD.

The setup program is implemented as a standard Windows wizard. Each window contains a set of buttons to control the installation process. Provided below is the brief description of their purpose:

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

A detailed discussion of each step of the package installation is provided below.

STEP 1. VERIFYING THAT THE SYSTEM MEETS THE INSTALLATION REQUIREMENTS

Before installing Kaspersky Anti-Virus on the computer, the wizard will verify that the computer meets the minimum requirements. It will also verify that you have the rights required to install software.

If any of the requirements is not met, the corresponding notice will be displayed on the screen. We recommend that you install any required updates using the **Windows Update** service, and the required programs, before attempting to install Kaspersky Anti-Virus again.

STEP 2. INSTALLATION START WINDOW

If your system meets the implied requirements completely, immediately after the installation file is launched, the start window will open on the screen displaying the information on the start of Kaspersky Anti-Virus installation.

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

STEP 3. VIEWING THE LICENSE AGREEMENT

The application's next dialog box contains the license agreement between you and Kaspersky Lab. Read it carefully, and if you agree with all terms and conditions of the agreement, select the **I accept the terms of the License Agreement** option and click the **Next** button. The installation will continue.

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

STEP 4. SELECTING INSTALLATION FOLDER

Next step of Kaspersky Anti-Virus installation defines the folder to install the application in. The default path is as follows:

- **<Drive> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Servers MP4** – for 32-bit systems.
- **<Drive> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Servers MP4** – for 64-bit systems.

You can specify a different folder by clicking the **Browse** button and selecting a folder in the standard folder selection window, or by entering the folder's path in the entry field provided.

Please note that if you manually enter the full path to the installation folder, its length should not exceed 200 characters, and the path should not contain special characters.

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

STEP 5. USING APPLICATION SETTINGS SAVED AFTER PREVIOUS INSTALLATION

At this step, you will be offered to specify if you wish to use protection settings and application databases in application's operation if those objects have been saved on your computer after the previous version of Kaspersky Anti-Virus 6.0 had been removed.

Let us take a closer look at how to enable the features described above.

If a previous version (build) of Kaspersky Anti-Virus had been installed on your computer, and you have saved the application databases after it had been removed, then you can integrate them into the version you are installing. To do so, check the **Application databases** box. Databases included in the installation package will not be copied on the server.

To use the protection settings that you have modified in a previous version and saved on your computer, check the **Application settings** box.

STEP 6. SELECTING THE TYPE OF THE INSTALLATION

At this step, you should define the completeness of application installation. There are two installation options:

Complete. In this case, all components of Kaspersky Anti-Virus will be installed on your server. To get acquainted with further steps of the installation, please refer to Step 8.

Custom. In this case, you will be offered to select which of the application components you wish to install. For more details see Step 7.

To select the installation mode, click the corresponding button.

STEP 7. SELECTING APPLICATION COMPONENTS FOR THE INSTALLATION

This step will be performed only if you selected the **Custom** installation option.

Before starting the custom installation, you should select which of Kaspersky Anti-Virus components you wish to install. By default, the File Anti-Virus component, virus scan component, and Network Agent connector to manage the application remotely via Kaspersky Administration Kit, are selected for the installation.

To select a component for further installation, you should open the menu by left-clicking on the icon next to the component name and select the **This feature will be installed on the local hard drive** item. The lower part of this installation program window displays the information about which type of protection is provided by the component you have selected, and how much storage space is required for its installation.

For detailed information about available disk space on your computer, click the **Volume** button. The information will be displayed in the window that will open.

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

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

STEP 9. SEARCHING FOR OTHER ANTI-VIRUS APPLICATIONS

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

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

You can choose whether to remove them automatically or manually, using the controls located below the list of detected anti-virus programs (only Kaspersky Lab's products will be removed automatically).

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

STEP 10. FINAL PREPARATION FOR INSTALLATION

This step completes the preparation for installing the application on your server.

At the initial installation of Kaspersky Anti-Virus 6.0, it is recommended not to uncheck the **Protect the installation process** box. The enabled protection of modules allows performing the correct procedure of installation rollback if some errors occur during the application installation. When you retry the installation of an application, we recommend that you uncheck this box.

If the application is being remotely installed using **Windows Remote Desktop**, you are advised to uncheck the **Protect the installation process** box. Otherwise, the installation procedure may be carried out incorrectly or not completed at all.

If you want the exclusions recommended for servers by Microsoft to be automatically added to the list of exclusions, check the **Exclude areas recommended by Microsoft from virus scan**.

If you want the path to avp.com to be added to the environmental variable %Path% after the installation, check the **Add path to avp.com to system variable %PATH%** box.

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

When installing Kaspersky Anti-Virus components, which intercept network traffic, current network connections are terminated. Most terminated connections are resumed after some time.

STEP 11. COMPLETING THE INSTALLATION

The **Installation complete** window contains information on completing the installation of Kaspersky Anti-Virus on the computer.

To run the Initial Configuration Wizard, click the **Next** button.

If a reboot is required for the installation to complete successfully, the special notification will be displayed on the screen.

APPLICATION INSTALLATION FROM THE COMMAND LINE

➤ To install Kaspersky Anti-Virus 6.0 for Windows Servers MP4, type the following in the command line:

```
msiexec /i <package_name>
```

The installation wizard will run (see section "Installation using the Installation Wizard" on page [16](#)). When the application is installed, the reboot is required.

➤ To install the application in non-interactive mode (without launching the installation wizard), type the following:

```
msiexec /i <package_name> /qn
```

In this case, the computer should be rebooted manually when the application installation is complete. To reboot the computer automatically, type the following in the command line:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Note that the automatic reboot can only be done in the non-interactive installation mode (with the /qn key).

➤ To install the application with a password, which confirms the right to remove the application, type the following:

```
msiexec /i <package_name> KLUNINSTPASSWD=***** – when installing the application in interactive mode;
```

`msiexec /i <package_name> KLUNINSTPASSWD=***** /qn` – when installing the application in non-interactive mode without rebooting the computer;

`msiexec /i <package_name> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn` – when installing the application in non-interactive mode and then rebooting the computer.

When installing Kaspersky Anti-Virus in non-interactive mode, the `setup.ini` file reading is supported; the file contains general settings for the installation of the application, `install.cfg` configuration file (see section Import of protection settings on page 107), and license key file. Note that those files should be located in the same folder as Kaspersky Anti-Virus installation package.

INSTALLATION FROM GROUP POLICY OBJECT EDITOR

Using **Group Policy Object editor** you can install, update and remove Kaspersky Anti-Virus on enterprise workstations making part of the domain, without using Kaspersky Administration Kit.

INSTALLING THE APPLICATION

➤ *To install Kaspersky Anti-Virus, please do the following:*

1. Create a shared network folder on the computer, which functions as domain controller, and place Kaspersky Anti-Virus installation package in *MSI* format into it.

Additionally, in this directory you can place the `setup.ini` file, which contains the list of settings for Kaspersky Anti-Virus installation, the `install.cfg` configuration file (see section Import of protection settings on page 107), and a license key file.

2. Open **Group Policy Object editor** from the standard MMC console (for detailed information on how to work with this editor please refer to Microsoft Windows Server help system).
3. Create a new package. To do so, select **Group Policy Object / Computer configuration/ Program configuration / Software installation** from the console tree, and use the **Create / Package** command from the context menu.

In the window that will open, specify the path to the shared network folder that stores Kaspersky Anti-Virus installation package. In the **Program deployment** dialog box, select the **Assigned** setting, and click the **OK** button.

The group policy will be applied to each workstation at the next registration of computers in the domain. As a result, Kaspersky Anti-Virus will be installed on all computers.

DESCRIPTION OF SETUP.INI FILE SETTINGS

The `setup.ini` file located in the directory of Kaspersky Anti-Virus installation package, is used when installing the application in non-interactive mode from the command line or Group Policy Object editor. This file includes the following settings:

[Setup] – general settings for application installation.

- **InstallDir**=<path to application installation folder>.
- **Reboot**=yes|no – defines whether the computer should reboot when the application installation is complete, or not (reboot does not run by default).
- **SelfProtection**=yes|no – defines if Kaspersky Anti-Virus Self-Defense should be enabled during the installation (Self-Defense is enabled by default).

[Components] – selection of application components to be installed. If this group contains no components, the application will be installed in its entirety.

- **FileMonitor=yes|no** – File Anti-Virus component installation.

[Tasks] – enabling Kaspersky Anti-Virus tasks. If no task is specified, all tasks will be enabled after the installation. If at least one task is specified, the tasks that have not been listed will be disabled.

- **ScanMyComputer=yes|no** – full scan task.
- **ScanStartup=yes|no** – quick scan task.
- **Scan=yes|no** – scan task.
- **Updater=yes|no** – update task for application databases and program modules.

The 1, on, enable, enabled values may be used instead of the **yes** value; the 0, off, disable, disabled values may be used instead of the **no** value.

UPDATING APPLICATION VERSION

➔ To update the version of Kaspersky Anti-Virus, please do the following:

1. Place the installation package that contains Kaspersky Anti-Virus updates in .msi format, in a shared network folder.
2. Open **Group Policy Object editor** and create a new package using the procedure described above.
3. Select the new package from the list and use the **Properties** command in the context menu. Select the **Updates** tab in the window of package properties, and specify the package, which contains the installation package of previous Kaspersky Anti-Virus version. To install an updated version of Kaspersky Anti-Virus saving protection settings, select the option of installation over the existing package.

The group policy will be applied to each workstation at the next registration of computers in the domain.

Please note that computers running under Microsoft Windows 2000 Server do not support Kaspersky Anti-Virus update via the Group Policy Object editor.

REMOVING THE APPLICATION

➔ To remove Kaspersky Anti-Virus, please do the following:

1. Open the **Group Policy Object Editor**.
2. Select **Group_Policy_Object / Computer configuration/ Program configuration/ Software installation** in the console tree.

Select Kaspersky Anti-Virus package from the list of packages, open the context menu, and execute the **All tasks/ Remove** command.

In the **Removing applications** dialog box, select **Immediately remove this application from computers of all users** for Kaspersky Anti-Virus to be removed at the next reboot.

GETTING STARTED

One of the main goals of Kaspersky Lab in creating Kaspersky Anti-Virus was to provide the optimum configuration of the application.

For the user's convenience, we have brought the preliminary configuration stages together in the unified interface of the Initial Configuration Wizard which starts upon the completion of the application installation procedure. By following the Wizard's instructions, you can activate the program, configure settings for updates and virus scan tasks launch, password-protect access to the application.

After completing installation and starting the program, we recommend taking the following steps:

- Evaluate the current protection status (see section "Security management" on page [28](#)) to make sure that Kaspersky Anti-Virus ensures the appropriate level of security.
- Update the application (see section Updating the application on page [26](#)) (unless it has been done using the setup wizard, or automatically immediately after the application had been installed).
- Scan the server (see section "Scanning computer for viruses" on page [26](#)) for viruses.

IN THIS SECTION

Initial Configuration Wizard.....	22
Scanning computer for viruses	26
Updating the application	26
Managing licenses.....	27
Security management.....	28
Pause protection	29
Eliminating problems. User technical support.....	29
Creating a trace file	29
Configuring application settings.....	30
Application operation reports. Data files	30

INITIAL CONFIGURATION WIZARD

Kaspersky Anti-Virus Configuration Wizard starts at the end of application installation. It is designed to help you configure the initial application settings, based on the features and tasks of your computer.

The Configuration Wizard interface is designed like a standard Microsoft Windows Wizard and consists of a series of steps that you can browse using the **Back** and **Next** buttons, or complete using the **Finish** button. To stop the wizard at any step, use the **Cancel** button.

To make complete installation of the application on the computer, all steps of the wizard's procedure should be taken. If the wizard's operation has been interrupted for some reasons, the values for the settings that had been already specified, will not be saved. At the next attempt of running the application, the Initial Configuration Wizard runs again thus requiring to edit the settings again.

USING THE OBJECTS SAVED FROM THE PREVIOUS VERSION

This wizard window appears when you install the application over the previous version of Kaspersky Anti-Virus. You are offered to choose which data used in the previous version should be imported to the new version. These might include quarantined or backup objects, or protection settings.

To use those data in the new version of the application, check all the necessary boxes.

ACTIVATING THE APPLICATION

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

The key file contains service information required for Kaspersky Anti-Virus to be fully functional as well as additional data:

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

Depending on whether you already have a key file, or will receive one from Kaspersky Lab's server, you will have the following options for activating Kaspersky Anti-Virus:

- Online activation (see page [24](#)). Select this activation option if you have purchased a commercial version of the application, and you have been provided an activation code. You can use this code to obtain a key file providing access to the application's full functionality throughout the effective term of the license.
- Activating trial version (see page [24](#)). Use this activation option if you want to install the trial version of the application before making the decision to purchase a commercial version. You will be provided a free key file valid for a term specified in the trial version license agreement.
- Activation with a license key file obtained earlier (see section "Activating using a key file" on page [24](#)). Activate the application using Kaspersky Anti-Virus 6.0 key file obtained earlier.
- Activate later. If you select this option, you will skip the activation stage. The application will be installed on your computer, and you will have access to all the application's features, except for updates (only one application update will be available, immediately after the installation). The **Activate later** option will only be available at the first startup of the Activation Wizard. At further wizard launches, if the application is already activated, the **Delete key file** option is available to perform the deletion.

If either of the first two application activation options is selected, the application will be activated via Kaspersky Lab's web server, which requires the Internet connection to link to. Before starting the activation, please verify and edit network connection settings as required in the window that will open by clicking the **LAN Settings** button. For more details on network settings, please contact your network administrator or Internet provider.

If at the time of installation no Internet connection is available, you can perform the activation later, using the application interface or connecting to the Internet from a different computer and obtaining a key, using an activation code received by registering on the Kaspersky Lab's Technical Support Service website.

You can also activate the application using Kaspersky Administration Kit. To do so, you should create a key file installation task (see page [121](#)) (for more details please refer to the Kaspersky Administration Kit help guide).

SEE ALSO

Online activation[24](#)

Obtaining a key file[24](#)

Activation using a key file[24](#)

Completing the activation[25](#)

ONLINE ACTIVATION

Online activation is performed by entering an activation code that you receive by email when you purchase Kaspersky Anti-Virus via the Internet. If you purchase the boxed application (retail version), the activation code will be printed on the envelope containing the installation disk.

ENTERING THE ACTIVATION CODE

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

Enter your personal information in the bottom part of the window: full name, email address, and country and city of residence. This information may be necessary to identify a registered user if, for example, his or her license data have been lost or stolen. In this case, you can obtain another activation code using your personal information.

OBTAINING A KEY FILE

The Configuration Wizard connects to Kaspersky Lab's internet servers and sends your registration data, including the activation code and your contact information. Once the connection is established, the activation code and contact information will be checked. If the activation code has passed the verification successfully, the Wizard receives a key file which then will be installed automatically. By the end of the activation, the window with detailed information on the obtained license will open.

If the activation code has not passed the verification, a relevant notification will pop up on the screen. If this happens, contact the software vendor from whom you purchased the application for information.

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

ACTIVATING THE TRIAL VERSION

Use this activation option if you want to install a trial version of Kaspersky Anti-Virus before making the decision to purchase a commercial version. You will be provided with a free license, which will be valid for the term specified in the trial version license agreement. Once the license expires, you will not be able to activate the trial version again.

ACTIVATION USING A KEY FILE

If you have a key file, you can use it to activate Kaspersky Anti-Virus. To do so, use the **Browse** button and select the file path for the file with the *.key* extension.

After you have successfully installed the key, you will see the information about the license in the bottom part of the window: license number, license type (commercial, beta, trial, etc.), license expiration date, and number of hosts.

COMPLETING THE ACTIVATION

The Configuration Wizard will inform you that Kaspersky Anti-Virus has been successfully activated. Additionally, information about the license is provided: license number, type (commercial, beta, trial, etc.), expiration date, and number of hosts.

UPDATE SETTINGS CONFIGURATION

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

- **Automatically.** Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scanning frequency may increase during anti-virus outbreaks and decrease when they are over. If new updates are found, Kaspersky Anti-Virus downloads and installs them on the computer. This is the default mode.
- **Every 2 hour(s)** (frequency may vary depending on the schedule settings). Updates will run automatically according to the schedule created. You can modify the schedule settings in another window by clicking the **Change** button.
- **Manually.** If you select this option, you will run application updates on your own.

Note that the application databases and modules included with the installation package may be outdated by the time you are installing the application. That is why we recommend you obtaining the latest updates of the application. To do so, click the **Update now** button. Then Kaspersky Anti-Virus will download the necessary updates from update sites and will install them on your computer.

If you wish to switch to configuring updates (specify network settings, select an update source, run an update from a specific user account, or enable update download to a local source), click the **Settings** button.

CONFIGURING VIRUS SCAN SCHEDULE

Scanning selected areas for malicious objects is one of the key tasks in protecting the computer.

When you install Kaspersky Anti-Virus, three default virus scan tasks are created. In this window, the Configuration Wizard asks you to select a scan task run mode:

Full Scan

A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded at startup, system backup, email databases, hard drives, removable storage media, and network drives. You can change the schedule settings in the window that will open by clicking the **Change** button.

Quick Scan

Virus scan of operating system startup objects. You can change the schedule settings in the window that will open by clicking the **Change** button.

RESTRICTING ACCESS TO THE APPLICATION

Since a server may be used by several people with varying levels of computer literacy, and due to malware which can disable the computer protection, you are offered to restrict access to Kaspersky Anti-Virus using a password. Using a password can protect the application from unauthorized attempts to disable protection, change the settings, or uninstall the application.

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

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

- **All operations (except notifications of dangerous events)**. The password will be requested if the user attempts to take any action on the application, apart from responding to notifications about the detection of dangerous objects.
- **Selected operations:**
 - **Configuring application settings** – request password if a user attempts to modify Kaspersky Anti-Virus settings.
 - **Closing application** – the password will be requested when the user attempts to exit the application.
 - **Disabling protection components and stopping scan tasks** – request the password when the user attempts to disable File Anti-Virus or stop a virus scan task.
 - **Disabling Kaspersky Administration Kit policy** – request the password if the user attempts to remove the computer from the scope of policies and group tasks (when operating via Kaspersky Administration Kit).
 - **Upon application uninstall** – request the password if the user attempts to remove the application from the computer.

FINISHING THE CONFIGURATION WIZARD

In the last window of the wizard, you will see a message saying that Kaspersky Anti-Virus has been installed and configured successfully. You can start the application immediately by checking **Start application**.

If something went wrong during installation, such as an incompatibility problem with other antivirus applications, you will be asked to restart your computer.

SCANNING COMPUTER FOR VIRUSES

Malware developers make every effort to conceal its actions, and therefore you may not notice the presence of malware on your computer.

Once Kaspersky Anti-Virus is installed on your computer, it automatically performs the **Quick Scan** task on your computer. This task searches for and neutralizes harmful programs in objects loaded during operating system startup.

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

➔ *To start / stop a virus scan task, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. Click the **Start scan** button to start the scan. If you need to stop the task execution, click the **Stop scan** button while the task is in progress.

UPDATING THE APPLICATION

You will need an Internet connection to update Kaspersky Anti-Virus.

Kaspersky Anti-Virus installation package includes the databases, which contain threat signatures. At the moment the application is installed, these databases may turn out to be obsolete, since Kaspersky Lab updates both the application databases and the application modules on a regular basis.

When Initial Configuration Wizard is active, you can select the update run mode. By default, Kaspersky Anti-Virus automatically checks for updates on Kaspersky Lab's servers. If the server contains a fresh set of updates, Kaspersky Anti-Virus will download and install them in the silent mode.

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

➔ *To update Kaspersky Anti-Virus by yourself, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. Click the **Start update** button.

MANAGING LICENSES

Kaspersky Anti-Virus requires a license to operate. You are provided with a license when you purchase the product. It gives you the right to use the product as soon as you activate it.

Without a license, if the trial version of the application has not been activated, Kaspersky Anti-Virus will run in one-update mode. The application will not download any new updates.

If a trial version of the application has been activated, Kaspersky Anti-Virus will not run after the free license expires.

When the commercial license expires, the application will continue working, except that you will not be able to update application databases. As before, you will be able to scan your computer for viruses and use the protection components, but only using the databases that you had when the license expired. We cannot guarantee that you will be protected from viruses that surface after your program license expires.

To avoid infecting your computer with new viruses, we recommend renewing your license for Kaspersky Anti-Virus. Two weeks before the license expiration, the application notifies you about it. During some period, a corresponding message will be displayed each time the application is launched.

General information on the license currently in use (active and additional licenses if the latter has been installed) is shown in the **License** section of the main window of Kaspersky Anti-Virus: license type (full, trial, beta), maximum number of hosts, license expiration date, and number of days to the expiration date. For more details about the license please click the link with the license type currently in use.

To view the provision of the application license agreement, click the **View End User License Agreement** button.

To remove the license, click the **Add / Delete** button and follow the instructions of the wizard that will open.

Kaspersky Lab has special pricing offers on license renewal for our products. Check for special offers on the Kaspersky Lab's website.

➔ *To purchase or renew a license, please do the following:*

1. Purchase a new key file or an activation code. Use the **Purchase license** (if the application has not been activated) or **License renewal** button. On the web page that will open you will be provided with detailed information on the terms of purchasing the key from Kaspersky Lab eStore or from authorized distributors. If you purchase online, a key file or an activation code will be mailed to you at the address specified in the order form once payment has been made.
2. Activate the application. Use the **Add / Delete** button in the **License** section of the main application window, or use the **Activate** command from the application context menu. This will start the Activation Wizard.

SECURITY MANAGEMENT

Problems in computer protection are indicated by the computer protection status (see section "Main application window" on page 33), which is displayed by changes in color of the protection status icon and of the panel on which it is located. Once problems appear in the protection, you are advised to solve them.



Figure 1. Current status of the computer protection

You can view the list of problems occurred, their description and possible ways of solving them, via Security Wizard (see figure below) which can be activated by clicking the **Fix** link (see figure above).

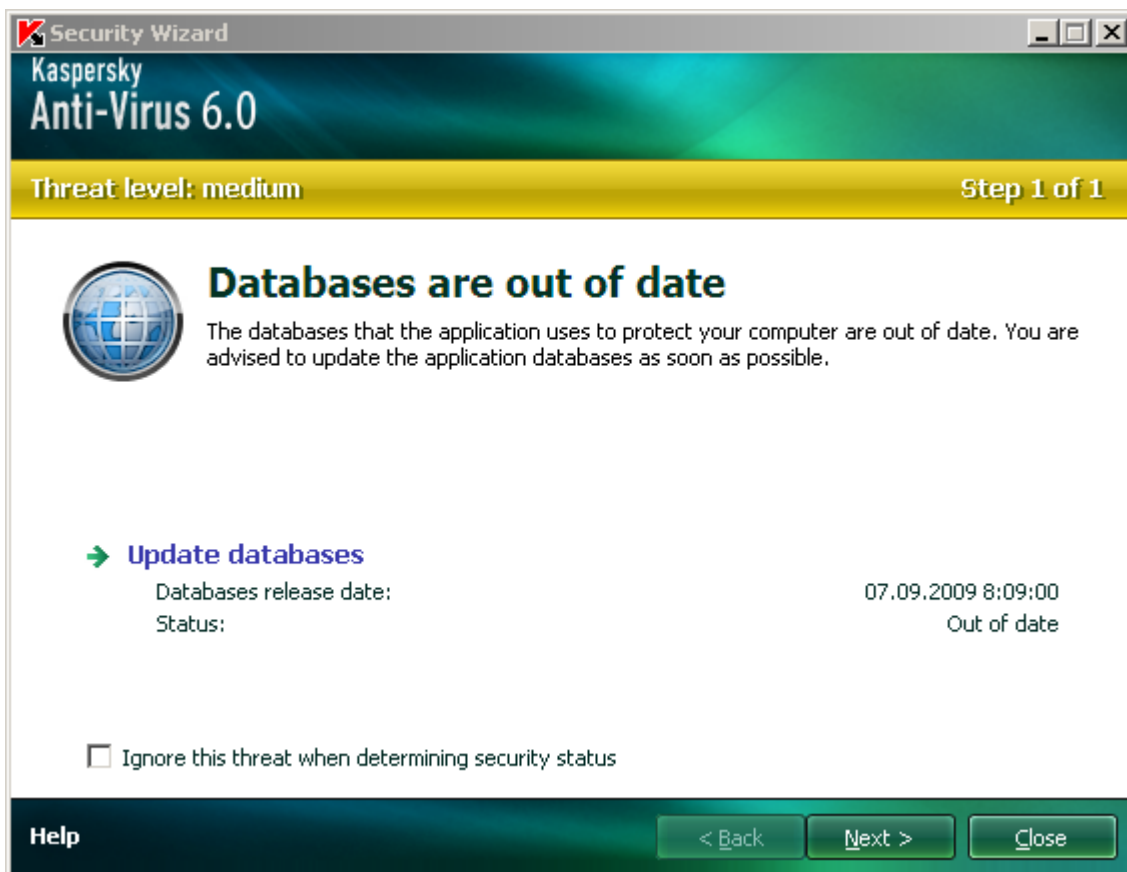


Figure 2. Solving security problems

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

- *Eliminate immediately.* Using the appropriate links, you can switch to fixing the problem, which is the recommended action.
- *Postpone elimination.* If, for any reason, immediate elimination of the problem is not possible, you can put off this action and return to it later. Check the **Ignore this threat when determining security status** box for the threat not to impact the current protection status.

Note that this option is not available for serious problems. Such problems include, for example, malicious objects that were not disinfected, crashes of one or several components, or corruption of the application files. Problems like these should be eliminated as quickly as possible.

PAUSING PROTECTION

Protection pausing consists in temporary disabling of File Anti-Virus.

➤ *To pause Kaspersky Anti-Virus, please do the following:*

1. In the application's context menu, select the **Pause Protection** item.
2. In the **Pause protection** window that will open, select the time period over which you wish the protection to be enabled, from the suggested options.

ELIMINATING PROBLEMS. USER TECHNICAL SUPPORT

If problems occur with the operation of Kaspersky Anti-Virus, the first place to check for help in for solving the problem is the Help system. The second place is the Kaspersky Lab Knowledge Base (<http://support.kaspersky.com>). The *Knowledge Base* is a separate section of the Technical Support web site, and comprises recommendations for Kaspersky Lab products as well as answers to frequently asked questions. Try to find an answer to your question or a solution to your problem with this resource.

➤ *To use the Knowledge Base, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Technical Support Service** link.

Another resource you can use to obtain information about working with the application is Kaspersky Lab users forum. It is another separate section of the Technical Support web site and it contains user questions, feedback and requests. You can view the main topics of the forum, leave feedback or find an answer to a question.

➤ *To open the users' forum, please do the following:*

1. Open the main application window.
2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **User Forum** link.

If you do not find a solution to your problem in Help, in the Knowledge Base, or at the User Forum, we recommend that you contact Kaspersky Lab's Technical Support.

CREATING A TRACE FILE

After installing Kaspersky Anti-Virus, some failures in the operating system or in the operation of individual applications may occur. The most likely cause is a conflict between the application and the software installed on your computer, or with the drivers of your computer's components. You may be asked to create a tracing file for Kaspersky Lab's specialists to successfully solve your problem.

➤ *To create the trace file:*

1. Open the main application window.

2. In the bottom part of the window, click the **Support** link.
3. In the **Support** window that will open, click the **Traces** link.
4. In the **Information for Technical Support Service** window that will open, use the dropdown list in the **Traces** section to select the tracing level. The tracing level should be set on the advice of the Technical Support specialist. If no instructions from the Technical Support are available, you are advised to set tracing level on **500**.
5. To start the tracing process, click the **Enable** button.
6. Reproduce the situation which caused the problem to occur.
7. To stop the tracing process, click the **Disable** button.

CONFIGURING APPLICATION SETTINGS

The application settings window (see page [69](#)) that can be accessed from the main window by clicking the **Settings** button, is designed for the quick access to Kaspersky Anti-Virus 6.0 settings.

APPLICATION OPERATION REPORTS. DATA FILES

The operation of File Anti-Virus and the execution of each virus scan and update task are recorded in a report (see page [84](#)). To view reports, use the **Reports** button in the lower right corner of the main window.

The objects that have been quarantined (see page [85](#)) or placed to the backup (see page [86](#)) by Kaspersky Anti-Virus, are called *application data files*. By clicking the **Detected** button, you can open the **Storage** window where you will be able to perform any actions you wish on those objects.

APPLICATION INTERFACE

Kaspersky Anti-Virus has a simple and easy-to-use interface. This chapter highlights its basic features:

- system tray icon;
- context menu;
- main window;
- notifications;
- Kaspersky Anti-Virus settings window.



IN THIS SECTION

Taskbar notification area icon.....	31
Context menu.....	32
Main application window.....	33
Notifications.....	34
Application settings window.....	35




TASKBAR NOTIFICATION AREA ICON

Right after installing Kaspersky Anti-Virus, its icon will appear in the system tray.

The icon is a sort of indicator for Kaspersky Anti-Virus operations. It also reflects the protection status and shows a number of basic functions performed by the application.

If the icon is active  (color), it means that protection is enabled on the server. If the icon is inactive  (black and white), this means that protection is disabled.

Kaspersky Anti-Virus icon changes depending on the operation being performed:

-  – a file that you or some program are opening, saving, or running is being scanned.
-  – Kaspersky Anti-Virus database and module update is in progress.
-  – an error has occurred in the operation of some Kaspersky Anti-Virus component.

The icon also provides access to the basic components of the application interface: context menu and main window.

To open the context menu, right-click on the application icon.

To open the Kaspersky Anti-Virus main window, click on the application icon.

CONTEXT MENU

You can run basic protection tasks from the context menu, which contains the following items:

- **Full Scan** – start a complete scan of your computer for malicious objects. Objects residing on all drives, including removable storage media, will be scanned.
- **Scan** – select objects and start the scan for viruses. By default, the list contains a number of objects, such as system memory, startup objects, email databases, all server drives, etc. You can enlarge the list, select other objects for scan and start virus scan.
- **Update** – start updates for application modules and databases of Kaspersky Anti-Virus and installs them on your computer.
- **Activate** – activate the application. To become a registered user with access to the application's full functionality and Technical Support, you have to activate your version of Kaspersky Anti-Virus. This menu item is only available if the application has not been activated.
- **Settings** – view and edit settings of Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus** – open the main application window.
- **Pause Protection / Resume Protection** – temporarily disable or enable File Anti-Virus. This menu option does not affect the application's updates, or the execution of virus scans.
- **Disable policy / Enable policy** – temporarily disable or enable policy when application is working via Kaspersky Administration Kit. This menu item allows removing the computer from the scope of policies and group tasks. This option is managed with a password (see section "Application access restriction" on page [79](#)). The menu item only appears if a password is set.
- **About** – display the window with information about the application.
- **Exit** – close Kaspersky Anti-Virus (when this option is selected, the application will be discarded from the computer's RAM).



Figure 3. Context menu

If a virus scan task is running, its name will be displayed in the shortcut menu with a percentage progress indication. After selecting a task, you can go to the report window to view current performance results.

MAIN APPLICATION WINDOW

The main application window can be divided into three parts:

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



Figure 4. Current status of the computer protection

There are three possible values of protection status: each of them is indicated with a certain color, similar to traffic lights. Green indicates that your computer's protection is at the correct level, while yellow and red colors indicate that there are security threats in the system configuration or in Kaspersky Anti-Virus operation. In addition to malicious programs, threats include, for example, out-of-date application databases.

Security threats should be eliminated as they appear. To obtain detailed information about them and to eliminate them quickly, use the **Fix** link (see figure above).

- The left part of the window provides quick access to any function of the application, including virus scan tasks, updates, etc.

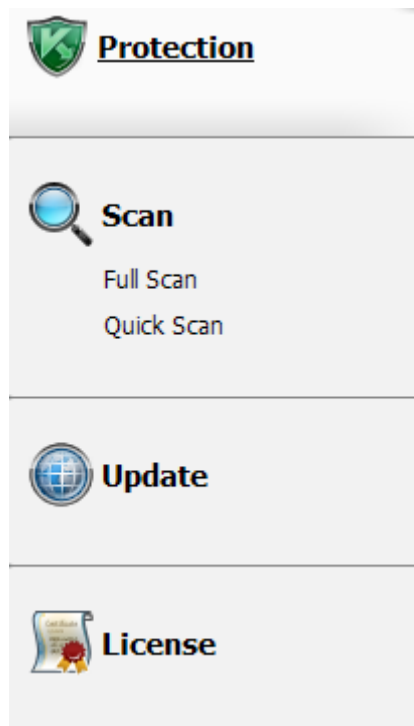


Figure 5. Left part of the main window

- The right part of the window contains information about the application's function selected in the left part, allows configuring its settings, provides tools for executing virus scan tasks, retrieving updates, etc.

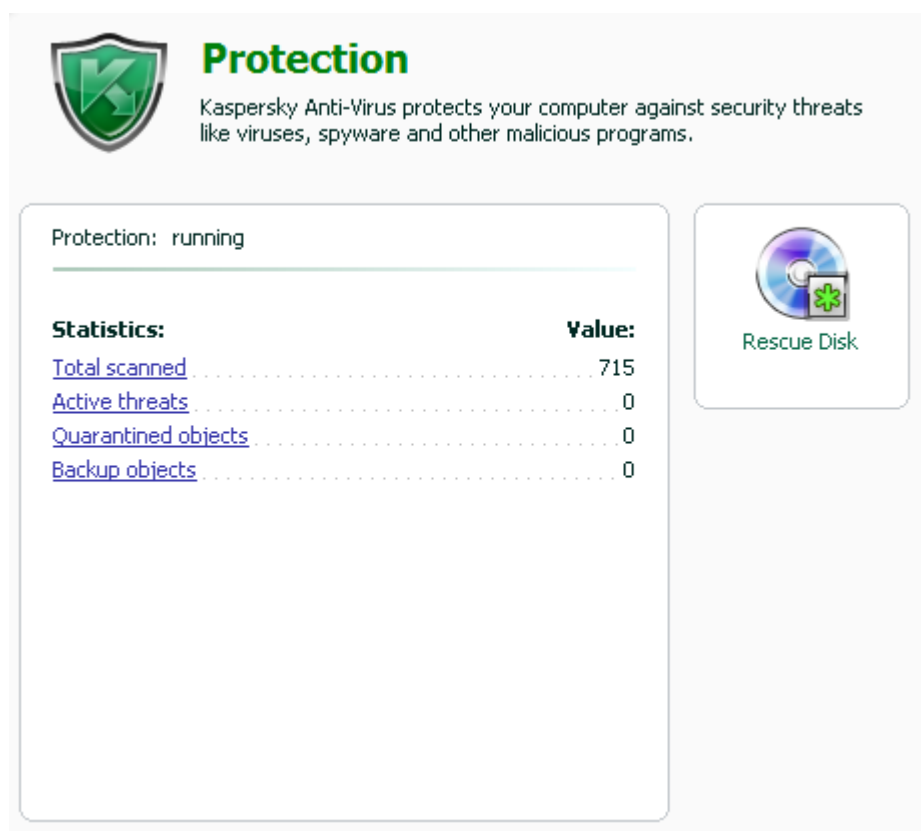


Figure 6. Right part of the main window

Additionally, you can use the following options:

- The **Settings** button – to open the application settings window (see page [69](#)).
- The **Help** link – to open Kaspersky Anti-Virus Help.
- The **Detected** button – to work with application datafiles (see page [83](#)).
- The **Reports** button – to open the reports on the application components' operation (see page [84](#)).
- The **Support** link – to open the window containing the information about the system and the links to Kaspersky Lab's information resources (see page [29](#)) (Technical Support service site, forum).

NOTIFICATIONS

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

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

- **Alarm.** An event of critical importance has occurred, such as a virus has been detected. You should immediately decide how to deal with this threat. This type of notification is color-coded in red.
- **Warning.** A potentially dangerous event has occurred, such as a potentially dangerous object has been detected. You should decide how dangerous you think this event is. This type of notification is color-coded in yellow.

- **Info.** This notification gives information about non-critical events. Minor notifications are color-coded in green.

SEE ALSO

Types of notifications.....[98](#)

APPLICATION SETTINGS WINDOW

You can open the Kaspersky Anti-Virus settings window from the main window. To do so, click the **Settings** button in the top part of the main window.

The settings window is designed like the main window:

- the left part of the window gives you quick and easy access to the settings for File Anti-Virus, virus scan tasks, update tasks and program options;
- the right part of the window contains a list of settings for the File Anti-Virus component, a task, etc., selected in the left part of the window.

SEE ALSO

Configuring application settings.....[69](#)

FILE ANTI-VIRUS

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

By default, File Anti-Virus scans only new or modified files. A collection of settings called security level determines the way of scanning files. If File Anti-Virus detects a threat, it will perform the preset action.

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

- protection scope settings;
- settings that determine the scan method used;
- settings that determine the scan of compound files (including scan of large compound files);
- settings that determine the scan mode;
- settings used to pause the component's operation (by schedule; during the operation of selected applications).

➡ *To modify File Anti-Virus settings:*

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

Component operation algorithm	37
Changing security level	38
Changing actions to be performed on detected objects.....	38
Creating a protection scope.....	39
Using heuristic analysis	40
Scan optimization	41
Scan of compound files	41
Scanning large compound files	41
Changing the scan mode.....	42
Scan technology.....	42
Pausing the component: creating a schedule.....	43
Pausing the component: creating a list of applications.....	43
Restoring default protection settings	43
File Anti-Virus statistics	44
Delayed object treatment.....	44

COMPONENT OPERATION ALGORITHM

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

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

1. The component intercepts every attempt by the user or by any program to access any file.
2. File Anti-Virus scans the iChecker and iSwift databases for information about the intercepted file and determines if it should scan the file, basing on the information retrieved.

The scan includes the following steps:

- The file is scanned for viruses. Objects are detected by comparing them with the application databases. The database contains descriptions of all malicious programs and threats currently known, and methods for processing them.
- After the analysis you have the following available courses of action for Kaspersky Anti-Virus:
 - a. If malicious code is detected in the file, File Anti-Virus blocks the file, creates a *backup* copy, and attempts to perform disinfection. After the file is successfully disinfected, it becomes operable to the user. If disinfection fails, the file is deleted.

- b. If potentially malicious code is detected in the file (but the maliciousness is not absolutely guaranteed), the file proceeds to disinfection and then is sent to the special storage area called *Quarantine*.
- c. If no malicious code is discovered in the file, it is immediately restored.

The application will notify you when an infected or a potentially infected file is detected. You should react to the notification by further processing the message:

- quarantine the object, allowing the new threat to be scanned and processed later using updated databases;
- delete the object;
- skip, if you are positive that the object cannot be malicious.

SEE ALSO

File Anti-Virus [36](#)

CHANGING SECURITY LEVEL

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

- If the computer has a high chance of becoming infected, it is necessary to select the high security level.
- Recommended level provides an optimum balance between efficiency and security, being suitable for most cases.
- While working in a protected environment (for example, in a corporate network with centralized security management) or with resource-consuming applications, it is recommended selecting the low security level.

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

If none of the preset levels meet your needs, you can configure the File Anti-Virus settings by yourself. As a result, the security level's name will change to **Custom**. To restore the default component's settings, select one of the preset security levels.

► To change the selected File Anti-Virus component security level, please do the following:

1. Open the main application window and click the **Settings** button in the top part of the window.
2. Select the required security level in the window that will open.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

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

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

If, while scanning a file for viruses, Kaspersky Anti-Virus discovers infected or possibly infected objects, the subsequent actions of File Anti-Virus depend on the objects status and the selected action.

By default, all infected files are subject to disinfection, and all potentially infected ones are subject to quarantine.

All possible actions are shown in the table below.

IF THE ACTION SELECTED WAS	WHEN A DANGEROUS OBJECT IS DETECTED
<input checked="" type="checkbox"/> Disinfect <input type="checkbox"/> Delete if disinfection fails	Access to the object is blocked and an attempt is made to disinfect it. A copy of the object is stored in Backup. If it is successfully disinfected, it is returned to the user for regular use. If the object could not be treated, it is moved to Quarantine. Relevant information is logged in the report. Later you can attempt to disinfect this object.
<input checked="" type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete if disinfection fails	Access to the object is blocked and an attempt is made to disinfect it. A copy of the object is stored in Backup. If it is successfully disinfected, it is returned to the user for regular use. If the object cannot be disinfected, it is deleted.
<input type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete	File Anti-Virus blocks access to the object and deletes it.
<input checked="" type="checkbox"/> Block infecting user for ... hours	<p>Blocks the current user's connection to the server if attempts are made to copy an infected or potentially infected object.</p> <p>This action can additionally be applied to actions related to processing the file (disinfecting or deleting).</p> <p>Note that if the user exits a session and logs into the system again, Kaspersky Anti-Virus will consider this a different connect and the ban will be lifted.</p>

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it and stores it in the Backup to allow later restoration or disinfection.

With the *potentially infected* status, the object is moved to Quarantine without an attempt to disinfect it.

➡ *To change the specified action to be performed on detected objects, please do the following:*

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
3. In the window that will open, in the **Action** section select the required action.

CREATING A PROTECTION SCOPE

A protection scope should be understood not only as the location of the objects to be scanned but also the type of files to be scanned. By default, Kaspersky Anti-Virus scans only potentially infectable files opened on any hard drive, network drive or removable media.

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

When selecting file types you should remember the following:

- There are a number of file formats that have a fairly low risk of having malicious code infiltrated into them and subsequently activated (for example, .txt). Conversely, there are formats that contain or can contain executable code, for instance .exe, .dll, .doc. The risk of activating malicious code in such files 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 have selected the **Files scanned by extension** option, such a file would be skipped by the scan. If the **Files scanned by format** setting has been selected, then, regardless of the extension, File Anti-Virus will analyze the file header, uncover that the file is an `.exe` file, and scan it for viruses.

When specifying the types of files to be scanned, you establish which file formats, sizes, and which drives will be scanned for viruses when opened, executed, or saved.

To make configuration easier, all files are divided into two groups: *simple* and *compound*. Simple files do not contain any objects (for example, `.txt` file). Compound files can include several objects, each of which may also have several nesting levels. Such objects can be archives, files containing macros, spreadsheets, emails with attachments, etc.

Remember that File Anti-Virus will scan only the files that are included in the protection scope created. Files that are not included in that scope will be available for use without scanning. This increases the risk of infection on your computer!

➤ *To edit the object scan list:*

- Open the main application window and click the **Settings** button in the top part of the window.
- In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
- In the window that will open, on the **General** tab, in the **Protection scope** section, click the **Add** button.
- In the **Select object to scan** window, select an object and click the **Add** button. Click the **OK** button after you have added all the objects you need.
- To exclude an object from the list of objects to be scanned, uncheck the boxes next to it.

➤ *To change the type of scanned objects:*

- Open the main application window and click the **Settings** button in the top part of the window.
- In the window that will open, click the **Customize** button.
- In the window that will open, on the **General** tab, in the **File types** section, select required settings.

USING HEURISTIC ANALYSIS

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

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

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

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

- Open the main application window and click the **Settings** button in the top part of the window.
- In the window that will open select the **File Anti-Virus** component and click the **Customize** button.

- In the window that will open, on the **Performance** tab, in the **Scan methods** section, check the **Heuristic analysis** box and specify the detail level for the scan.

SCAN OPTIMIZATION

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

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

- Open the main application window and click the **Settings** button in the top part of the window.
- In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
- In the window that will open, on the **Performance** tab, check the **Scan new and changed files only** box.

SCAN OF COMPOUND FILES

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 should be unpacked, which can significantly lower the scan speed.

Installer packages and files containing OLE objects are executed while being opened, which makes them more dangerous than archives. To protect your computer against execution of malicious code and, at the same time, increase the scan speed, disable archive scans and enable scans for this file type.

If a file with embedded OLE object is an archive, it will be scanned during unpacking. You can enable archive scan to scan files with embedded OLE objects before their unpacking. However, this will result in significant scan speed decrease.

By default, Kaspersky Anti-Virus scans only embedded OLE objects.

➤ *To modify the list of scanned compound files:*

- Open the main application window and click the **Settings** button in the top part of the window.
- In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
- In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, check the boxes for the types of compound files to be scanned.

SCANNING LARGE COMPOUND FILES

When large compound files are scanned, their preliminary unpacking may require a long time. You can shorten this time only if you perform the file scan in the background. If a malicious object is detected while working with such a file, the application will notify you about it.

To reduce the access delay time for compound files, disable the unpacking of files larger than the size you have specified. When files are extracted from an archive, they will always be scanned.

➤ *If you want the application to unpack large files in the background, please do the following:*

- Open the main application window and click the **Settings** button in the top part of the window.
- In the window that will open select the **File Anti-Virus** component and click the **Customize** button.

3. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
4. In the **Compound files** window, check the **Extract compound files in the background** box and specify the minimum file size value in the field below.

➤ *If you do not want the application to unpack large compound files, please do the following:*

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
3. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
4. In the **Compound files** window, check the **Do not unpack large compound files** box and specify the maximum file size value in the field below.

CHANGING THE SCAN MODE

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

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

➤ *To change the object scan mode:*

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
3. In the window that will open, on the **Additional** tab, in the **Scan mode** section, select the required mode.

SCAN TECHNOLOGY

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

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

For example, you have an archive file that the application has scanned and assigned the *not infected* status to it. The next time the application will skip this archive, unless it has been altered, or the scan settings have been changed. If the archive's structure has changed by adding a new object to it, or if the scan settings have changed, or if the application databases have been updated, the archive will be re-scanned.

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

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

➤ *To change the object scan technology:*

1. Open the main application window and click the **Settings** button in the top part of the window.

2. In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
3. In the window that will open, on the **Additional** tab, in the **Scan technologies** section, select the required setting value.

PAUSING THE COMPONENT: CREATING A SCHEDULE

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

➤ *To configure a schedule for pausing the component:*

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
3. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **On schedule** box and click the **Schedule** button.
4. In the **Pause task** window, specify the time (in 24-hour HH:MM format) for which the protection will be paused (**Pause task at** and **Resume task at** fields).

PAUSING THE COMPONENT: CREATING A LIST OF APPLICATIONS

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

Configuring the disabling of File Anti-Virus component if it conflicts with certain applications is an emergency measure! In case of conflicts in the component's operation, please contact Kaspersky Lab Technical Support Service (<http://support.kaspersky.com>). Support specialists can help you resolve simultaneous operation of Kaspersky Anti-Virus with the software on your computer.

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

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open select the **File Anti-Virus** component and click the **Customize** button.
3. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **At application startup** box and click the **Select** button.
4. In the **Applications** window, create a list of applications which will pause the component when running.

RESTORING DEFAULT PROTECTION SETTINGS

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

If you have modified the list of objects included in the protected zone when configuring File Anti-Virus settings, the application will ask you if you want to save that list for further use when restoring the initial settings.

➤ To restore the default protection settings and to save the modified list of objects included in the protected zone:

1. Open the main application window and click the **Settings** button in the top part of the window.
2. In the window that will open select the **File Anti-Virus** component and press the **Default level** button.
3. In the **Restore settings** window that will open, check the **Protection scope** box.

FILE ANTI-VIRUS STATISTICS

All operations carried out by File Anti-Virus are recorded in a special report. To view information on the component's operation, click the **Statistics** link. You will see a detailed report on the component operation, grouped on tabs:

- All dangerous objects detected during the file system protection process are listed on the *Detected* tab. Here you will find the full path to the location of each object and the status assigned to it by File Anti-Virus: if what malicious program infected the object was successfully established, it will be assigned the appropriate status. For example, virus, Trojan, etc. If the type of malicious impact cannot be exactly established, the object is assigned the *suspicious* status. The action applied to the object (detected, not found, disinfected) is also shown next to the status.

For this tab not to contain information about disinfected objects, uncheck the **Show disinfected objects** box.

- The complete list of events that have occurred while using File Anti-Virus is kept on the *Events* tab. Events can be of the following types:
 - *Information* (for example, object not processed, skipped by type).
 - *Warning* (for example, a virus is detected).
 - *Comment* (for example, archive is password-protected).

As a rule, informative messages are reference-type messages and are not of particular interest. You can disable display of informative messages. To do so, uncheck the **Show all events** box.

- *Scan statistics* appear on the appropriate tab. Here you will find the total number of objects scanned, and then special columns separately display how many objects out of the total number scanned are archives, how many of them are dangerous, how many have been disinfected, how many have been quarantined, etc.
- The settings that File Anti-Virus is running with are displayed on the *Settings* tab. Use the **Change settings** link to quickly configure the component.
- The *Banned users* tab displays a list of users whose computers have been banned when attempting to copy an infected or potentially infected files to the server.

DELAYED OBJECT TREATMENT

In Kaspersky Anti-Virus for Windows Servers, access to infected files is blocked if they are being disinfected and if deleted in cases where they could not be disinfected or deleted.

To regain access to blocked objects, you first have to try to disinfect them. If an object is successfully disinfected, it will be restored for regular use. If the object cannot be disinfected, you will be offered to *delete* or *skip* it. In the latter case, access to the file will be restored. However, this significantly increases the risk of infection on the server. It is strongly recommended not to skip malicious objects.

➤ To obtain access to the blocked objects for disinfecting them, please do the following:

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

2. In the window that will open, on the **Active threats** tab, select the required objects and click the **Neutralize all** link.

SEE ALSO

Changing actions to be performed on detected objects.....[38](#)

SERVER VIRUS SCAN

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 can scan separate items (files, folders, disks, removable media) or the entire computer for viruses. Scanning for viruses rules out the possibility of spreading the malicious code that has not been detected by File Anti-Virus for any reason.

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 comprises the following default virus scan tasks:

Scan

Scan of objects selected by the user. You can scan any object in the computer's file system.

Full Scan

A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded at startup, system backup, email databases, hard drives, removable storage media, and network drives.

Quick Scan

Virus scan of operating system startup objects.

By default, those tasks run with recommended settings. These settings may be modified, and tasks may be scheduled to run.

In addition, you can scan any object for viruses without creating a special scan task. An object to scan may be selected using the Kaspersky Anti-Virus interface or standard Microsoft Windows Server tools (for example, **Windows Explorer** or **Desktop**, etc.). Place the cursor on the desired object's name, right-click to open the Microsoft Windows context menu, and select the **Scan for viruses** option.



Figure 7. Microsoft Windows context menu

Additionally, following a scan you can view the scan report, which contains full information about events which occurred during the execution of the tasks.

➤ *To change the settings of any virus scan task, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, make the required changes in the settings for the task you have selected.

➤ To switch to the virus scan report, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. Click the **Reports** button.

IN THIS SECTION

Starting the virus scan	47
Creating a list of objects to scan	48
Changing security level	49
Changing actions to be performed on detected objects.....	49
Changing the type of objects to scan.....	50
Scan optimization	51
Scan of compound files	52
Changing the scan method.....	52
Scan technology	52
Computer performance during task execution.....	53
Pausing the task: creating a schedule	53
Pausing the component: creating a list of applications	54
Run mode: specifying an account	54
Run mode: creating a schedule	55
Features of scheduled task launch.....	55
Virus scan statistics	56
Assigning common scan settings for all tasks	56
Restoring default scan settings	56

STARTING THE VIRUS SCAN

You can start a virus scan task in one of the two following ways:

- from Kaspersky Anti-Virus context menu;
- from the main window of Kaspersky Anti-Virus.

Task execution information will be displayed in the main window of Kaspersky Anti-Virus.

In addition, you can select an object to be scanned with the help of standard tools of the Microsoft Windows operating system (for example, in the **Explorer** program window or on your **Desktop**, etc.).



Figure 8. Microsoft Windows context menu

➤ To start a virus scan task from the context menu, please do the following:

1. Right-click the application icon in the taskbar notification area.
2. Select the **Scan** item from the dropdown menu. In the main application window that will open, select the required **Scan (Full Scan, Quick Scan)** task. If required, configure the selected task and click the **Start scan** button.
3. Alternatively, you can select the **Full Scan** item from the context menu. This will start a full computer scan. The task progress will be displayed in the main window of Kaspersky Anti-Virus.

➤ To start the virus scan task from the main application window:

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. Click the **Start scan** button for selected section. The task progress will be displayed in the main application window.

➤ To start a virus scan task for a selected object from the Microsoft Windows context menu:

1. Right-click the name of the selected object.
2. Select the **Scan for viruses** item in the context menu that will open. The progress and the results of task execution will be displayed in the statistics window.

CREATING A LIST OF OBJECTS TO SCAN

Each virus scan task has its own default list of objects. To view a list of objects, select the task name (such as **Full Scan**) in the **Scan** section of the main application window. The list of objects will be displayed in the right part of the window.

Lists of objects to scan are already generated for default tasks created at the application installation.

For the user's convenience, you can add categories to the scan scope, such as user's mailboxes, RAM, startup objects, operating system backup, and files in the Kaspersky Anti-Virus Quarantine folder.

Besides, when you add a folder that contains embedded objects to the scan scope, you can edit the recursion. To do so, select the required object from the list of objects to scan, open the context menu, and use the **Include subfolders** option.

➤ To create a list of objects to scan, please do the following:

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. Click the **Add** link for the selected section.
4. In the **Select object to scan** window that will open, select an object and click the **Add** button. Click the **OK** button after you have added all the objects you need. To exclude any objects from the list of objects to scan, uncheck the boxes next to them. To remove an object from the list, select it and click the **Delete** link.

CHANGING SECURITY LEVEL

The security level is a preset collection of scan settings. Kaspersky Lab specialists distinguish three security levels. You should make the decision on which level to select based on your own preferences:

- If you suspect that your computer has a high chance of becoming infected, select the High security level.
- The recommended level is suitable in most cases, and is advised for using by Kaspersky Lab specialists.
- If you are using applications requiring considerable RAM resources, select the Low security level because the application puts least demand on system resources in this mode.

If none of the preset levels meet your needs, you can configure the scan settings yourself. As a result, the security level's name will change to **Custom**. To restore the default scan settings, select one of the preset security levels. By default, scan is set at the **Recommended** level.

➤ To change the defined security level, perform the following actions:

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, adjust the slider on the scale. By adjusting the security level, you define the ratio of scan speed and the total number of files scanned: the fewer files are subject to analysis for viruses, the higher the scan speed is. You can also click the **Customize** button and modify the required settings in the window that will open. The security level will change to **Custom**.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

If a virus scan identifies an object as infected or suspect, subsequent processing by the application depends on the status of the object and the action selected.

Based on the scan results, an object may be assigned one of the following statuses:

- the malicious program status (such as *virus*, *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.

By default, all infected files are subject to disinfection, and all potentially infected ones are placed to quarantine.

IF THE ACTION SELECTED WAS	WHEN A MALICIOUS / POTENTIALLY INFECTED OBJECT IS DETECTED
<input checked="" type="radio"/> Prompt for action when the scan is complete	The application will postpone processing of objects until the scan is complete. When the scan is complete, the program will prompt the user for actions for each of the files one after another.
<input checked="" type="radio"/> Prompt for action during scan	File Anti-Virus displays a warning message containing information about what malicious program has infected or potentially infected the file and gives you a choice of action.
<input checked="" type="radio"/> Do not prompt for action	The application creates a report with information about objects detected without processing them or notifying the user. This application mode is not recommended, because it leaves infected or potentially infected objects on your computer making infection virtually inevitable.
<input checked="" type="radio"/> Do not prompt for action <input checked="" type="checkbox"/> Disinfect	The application creates a report with information about objects detected without processing them or notifying the user. This application mode is not recommended, because it leaves infected or potentially infected objects on your computer making infection virtually inevitable.
<input checked="" type="radio"/> Do not prompt for action <input checked="" type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete if disinfection fails	The application attempts to disinfect the object without requesting any confirmation from the user. If the object cannot be disinfected, it will be deleted. A copy is saved in the Backup.
<input checked="" type="radio"/> Do not prompt for action <input type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete	The application deletes the object automatically.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it and stores it in the Backup to allow later restoration or disinfection.

With the *potentially infected* status, the object is moved to Quarantine without an attempt to disinfect it.

➤ *To change the specified action to be performed on detected objects, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the **Action** section, enter the required changes in the window that will open.

CHANGING THE TYPE OF OBJECTS TO SCAN

When specifying the type of objects to scan, you establish which file formats and sizes will be scanned for viruses when the selected virus scan runs.

When selecting file types you should remember the following:

- Certain file formats (such as *.txt*) have a fairly low risk of having malicious code infiltrated into them and subsequently activated. At the same time, there are formats that contain or may contain an executable code (such as *.exe*, *.dll*, *.doc*). The risk of penetration and activation of malicious code in such files is fairly high.
- Remember that an intruder can send a virus to your computer in a file with the *.txt* extension, whereas it is in fact an executable file renamed as *.txt* file. If you have selected the **Files scanned by extension** option, such a file will be skipped by the scan. If the **Files scanned by format** option has been selected, regardless the extension, the file protection will analyze the file header and may determine that the file is an *.exe* file. Such a file would be thoroughly scanned for viruses.

➤ *To change the type of scanned objects:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Scope** tab, in the **File types** section, select the required settings.

SCAN OPTIMIZATION

You can shorten the scan time and speed up Kaspersky Anti-Virus. This can be achieved by scanning only new files and those files that have altered since the last time they were scanned. This mode applies both to simple and compound files.

Additionally, you can impose a restriction on the scan length. Once the specified time period is elapsed, the file scan will be stopped. You can also limit the size of the file being scanned. The file will be skipped if its size exceeds the value you have set.

➤ *To scan only new and changed files, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Scope** tab, in the **Scan optimization** section, check the **Scan only new and changed files** box.

➤ *To impose a time restriction on the scan duration:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Scope** tab, in the **Scan optimization** section, check the **Stop scan if it takes longer than** box and specify the scan duration in the field next to it.

➤ *To limit the size of the file to scan, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Scope** tab, click the **Additional** button.
6. In the **Compound files** window that will open, check the **Do not unpack large compound files** box and specify the file size in the field next to it.

SCAN OF COMPOUND FILES

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

For each type of compound file, you can select to scan either all files or only new ones. To do so, use the link next to the name of the object. It changes its value when you left-click on it. If you select the scan new and changed files only scan mode, you will not be able to select which types of compound files are to be scanned.

➤ *To modify the list of scanned compound files:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Scope** tab, in the **Scan of compound files** section, select the required type of compound files to be scanned.

CHANGING THE SCAN METHOD

You can use *heuristic analysis* as the scan method. It analyzes the actions an object performs on the system. If its actions are typical of malicious objects, the object is likely to be classed as malicious or suspicious.

Additionally, you can set the detail level for heuristic analysis by moving the slider bar to one of the following positions: **light**, **medium**, or **deep**.

In addition to this scan method, you can use the Rootkit Scan. *Rootkit* is a set of tools that can hide malicious applications in your operating system. These utilities are injected into the system, hiding their presence and the presence of processes, folders and the registry keys of other malicious programs installed with the rootkit. If the scan is enabled, you can specify detailed level (advanced analysis) to detect rootkits. It will scan carefully for such programs by analyzing a large number of various objects.

➤ *To specify which scan method to use:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Additional** tab, in the **Scan methods** section, select the required scan technologies.

SCAN TECHNOLOGY

Additionally, you can specify the technology which will be used during the scan:

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

For example, you have an archive file which has been scanned by Kaspersky Anti-Virus and assigned the *not infected* status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If the archive's structure has changed by adding a new object to it, or if the scan settings have changed, or if the application databases have been updated, the archive will be re-scanned.

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

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

➔ *To use the object scan technology, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Additional** tab, in the **Scan technologies** section, enable the required technology.

COMPUTER PERFORMANCE DURING TASK EXECUTION

Virus scan tasks may be postponed to limit the load on the central processing unit (CPU) and disk storage subsystems.

Executing scan tasks increases the load on the CPU and disk subsystems, thus slowing down other applications. By default, if such a situation arises, Kaspersky Anti-Virus will pause virus scan tasks and release system resources for the user's applications.

However, there is a number of applications which will start immediately when CPU resources become available, and will run in the background. For the scan not to depend on the performance of those applications, system resources should not be conceded to them.

Note that this setting can be configured individually for every virus scan task. In this case, the configuration for a specific task has a higher priority.

➔ *To postpone the execution of scan tasks if it slows down other applications, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Additional** tab, in the **Scan methods** section, check the **Concede resources to other applications** box.

PAUSING THE TASK: CREATING A SCHEDULE

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

➤ *To configure the schedule for task pausing, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. Select the **Customize** item from the dropdown menu.
5. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **On schedule** box and click the **Schedule** button.
6. In the **Pause task** window, specify the time (in 24-hour HH:MM format) for which the protection will be paused (**Pause task at** and **Resume task at** fields).

PAUSING THE COMPONENT: CREATING A LIST OF APPLICATIONS

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

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

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. Select the **Customize** item from the dropdown menu.
5. In the window that will open, on the **Additional** tab, in the **Pause task** section, check the **At application startup** box and click the **Select** button.
6. In the **Applications** window, create a list of applications which will pause the component when running.

RUN MODE: SPECIFYING AN ACCOUNT

You can specify an account used by the application when performing a virus scan.

➤ *To start the task with the privileges of a different user account:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Security Level** section, click the **Customize** button.
5. In the window that will open, on the **Run mode** tab, in the **User** section, check the **Run task as** box. Specify the user name and password.

RUN MODE: CREATING A SCHEDULE

All virus scan tasks can be started manually, or by a schedule.

The default schedule setting for the tasks created when the program is installed is off. The exception is the quick scan task, which runs every time you start your computer.

When creating a schedule on tasks launch it is necessary to set the interval of the scans.

If it is not possible to start the task for any reason (for example, the computer was not on at specified time), you can configure the task to start automatically as soon as it becomes possible.

➤ *To edit a schedule for scan tasks:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, press the **Change** button in the **Run mode** section.
5. Make the required changes in the **Schedule** window that will open.

➤ *To configure automatic launches of skipped tasks:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, press the **Change** button in the **Run mode** section.
5. In the **Schedule** window that will open, in the **Schedule settings** section, check the **Run task if skipped** box.

FEATURES OF SCHEDULED TASK LAUNCH

All virus scan tasks can be started manually, or by a schedule.

Scheduled tasks feature an additional functionality, for example, you can check the *Pause scheduled scan when screensaver is inactive or computer is unlocked* box. This functionality postpones the task launch until the user has finished working on the computer. So, the scan task will not take up system resources during the work.

➤ *To launch scan tasks only when the computer isn't in use any more, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Full Scan, Quick Scan** section.
3. For the selected section, click the link with the preset security level.
4. In the window that will open, in the **Run mode** section, check the **Pause scheduled scan when screensaver is inactive or computer is unlocked** box.

VIRUS SCAN STATISTICS

General information on each virus scan task is shown in the statistics window. Here you can check how many objects have been scanned and how many hazardous and suspicious objects subject to processing have been detected. Additionally, here you can find information about the starting and completing time of the last task run and about the scan length.

General information on scan results is grouped on the following tabs:

- The *Detected* tab lists all dangerous objects detected when executing a task.
- The *Events* tab lists all events occurred when executing a task.
- The *Statistics* tab provides statistical data of scanned objects.
- The *Settings* tab provides the settings, which determine the way of executing a task.

If any errors have occurred during the scan, try running it again. If the next attempt returns an error, we recommend that you save the report on task results in a file using the **Save as** button. Then contact the Technical Support Service, and send the report file. Kaspersky Lab's specialists will certainly help you.

➤ *To view statistics of a virus scan task, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section, create a scan task, and launch it. The task progress will be displayed in the main window. Click the **Details** link to switch to the statistics window.

ASSIGNING COMMON SCAN SETTINGS FOR ALL TASKS

Each scan task is run according to its own settings. By default, the tasks created at the application installation are run with the settings recommended by Kaspersky Lab experts.

You can configure universal scan settings for all tasks. You will use a set of properties used to scan an individual object for viruses as a starting point.

➤ *To assign universal scan settings to all tasks, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Scan** section.
3. In the right part of the window, in the **Other task settings** section, click the **Apply** button. Confirm the universal settings that you have selected in the pop-up dialog box.

RESTORING DEFAULT SCAN SETTINGS

When editing task settings, you can always restore the recommended ones. They are considered optimal, recommended by Kaspersky Lab, and grouped in the **Recommended** security level.

➤ *To restore the default file scan settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.

3. For the selected section, click the link with the preset security level.
4. In the window that will open, click the **Default level** button in the **Security Level** section.

UPDATING THE APPLICATION

Keeping protection updated is a prerequisite of reliable protection. New viruses, Trojans, and malicious software emerge daily, so it is important to update the application regularly to keep your personal data constantly protected.

The application's update component downloads and installs the following updates on the server:

- **Application databases**

The protection of information is ensured by application databases. File Anti-Virus uses them to search for and disinfect harmful objects on the server. The databases are added to every hour with records of new threats. Therefore, you are advised to update them on a regular basis.

- **Application modules**

In addition to the application databases, you can also update the application modules. The update packages fix the application's vulnerabilities and add new or improve the existing functionality.

Kaspersky Lab update servers are the primary sources of Kaspersky Anti-Virus updates.

To successfully download updates from servers, your computer must be connected to the Internet. By default, the Internet connection settings are determined automatically. If the proxy server settings are not properly configured automatically, the connection settings can be set manually.

During an update, application modules and databases on your computer are compared to those in the update source. If your computer has the latest version of the databases and application modules, you will see a notification window confirming that your computer's protection is up to date. If the databases and modules on your computer differ from those on the update server, the application downloads only the incremental part of the updates. The fact that not all the databases and modules are downloaded significantly increases the speed of copying files and saves Internet traffic.

Before updating the databases, Kaspersky Anti-Virus creates backup copies of them, so that you can use it again in the future.

You might need the rollback option if, for example, the databases have become corrupted during the update process. You can easily roll back to the previous version and try to update the databases again.

You can copy the retrieved updates to a local source while updating the application. This service allows updating the databases and modules of the application on networked computers to save Internet traffic.

You can also configure automatic update startup.

The **Update** section displays the current status of the application databases.

You can view the updating report, which contains full information about events that have occurred during updating. You can also see the virus activity overview at www.kaspersky.com by clicking the **Virus activity review** link.

➤ *In order to edit the settings of any update task, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, make the required changes in the settings for the task you have selected.

➤ *To switch to update report, please do the following:*

1. Open the main window.

2. In the left part of the window, select the **Update** section.
3. Click the **Reports** button.

IN THIS SECTION

Starting the update	59
Rolling back the last update	60
Selecting an update source	60
Regional settings	61
Using a proxy server.....	61
Run mode: specifying an account	61
Run mode: creating a schedule	62
Selecting objects to update	62
Changing the update task's run mode	63
Updating from a local folder.....	63
Update statistics	64
Possible problems during the update	64

STARTING THE UPDATE

You can start the application update at any time. Updates are downloaded from the selected update source.

You can update Kaspersky Anti-Virus using one of the two supported methods:

- From the context menu.
- From the main application window.

Update information will be displayed in the main application window.

Note that the updates are distributed to a local source during the updating process, provided that this service is enabled.

➤ *To start Kaspersky Anti-Virus update from the context menu:*

1. Right-click the application icon in the taskbar notification area.
2. Select the **Update** item from the dropdown menu.

➤ *To start Kaspersky Anti-Virus update from the main application window:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. Click the **Start update** button. The task progress will be displayed in the main application window.

ROLLING BACK THE LAST UPDATE

At the start of the update process Kaspersky Anti-Virus creates a backup copy of the current databases and application modules. This allows the application to continue working, using the previous databases, if the update fails.

The rollback option is useful if, for example, part of the databases has been corrupted. Local databases can be corrupted by the user or by a malicious program, which is possible only if the application's self-defense is disabled. You can easily roll back to the previous databases and try to update the databases later.

➔ *To roll back to the previous database version:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. Click the **Roll back to the previous databases** link.

SELECTING AN UPDATE SOURCE

Update source is a resource containing updates for databases and application modules of Kaspersky Anti-Virus.

You can use the following as update sources:

- *Administration Server* is a centralized update repository located on the Kaspersky Administration Kit Administration Server (for more details see the Administrator's Guide for Kaspersky Administration Kit).
- *Kaspersky Lab's update servers* are special websites containing updates for the databases and application modules for all Kaspersky Lab's products.
- *FTP or HTTP servers, local or network folders* are local servers or folders that contain the latest updates.

If you do not have access to Kaspersky Lab's update servers (for example, your computer is not connected to the Internet), you can call the Kaspersky Lab main office at +7 (495) 797-87-00 or +7 (495) 645-79-39 to request contact information of Kaspersky Lab partners who can provide you with updates on floppy disks or ZIP disks.

You can copy the updates from a removable disk and upload them to an FTP or HTTP website, or save them in a local or network folder.

When requesting updates on removable media, please specify if you want to have the updates for application modules as well.

If you select a resource outside the LAN as an update source, you must have an Internet connection to update.

If several resources are selected as update sources, the application will try to connect to them in turn, starting at the top of the list and retrieving the updates from the first available source.

➔ *To choose an update source:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, in the **Update settings** section, click the **Configure** button.

5. In the window that will open, on the **Update source** tab, click the **Add** button.
6. Select an FTP or HTTP site, or enter its IP address, symbolic name or URL in the **Select update source** window that will open.

REGIONAL SETTINGS

If you use Kaspersky Lab update servers as update source, you can select the optimal server location when downloading updates. Kaspersky Lab servers are located in several countries. Choosing the Kaspersky Lab update server closest to you will let you save time and download updates faster.

➤ *To choose the closest server:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, in the **Update settings** section, click the **Configure** button.
5. In the window that will open, on the **Update Source** tab, in the **Regional settings** section, select the **Select from list** option and then select the country nearest to your current location from the dropdown list.

If you select the **Autodetect** option, the information on your location will be copied from your operating system's registry when updating.

USING A PROXY SERVER

If you are using a proxy server to connect to the Internet, you must configure its settings.

➤ *To configure the proxy server, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, in the **Update settings** section, click the **Configure** button.
5. In the window that will open, edit the proxy server settings on the **Proxy settings** tab.

RUN MODE: SPECIFYING AN ACCOUNT

Kaspersky Anti-Virus has a feature that can start program updates from another profile. By default, this service is disabled, and tasks are started using the account under which you are registered in the system.

Since the application can be updated from a source that you do not have access to (such as the network updates directory) or authorized user rights to the proxy server, you can use this feature to run application updates using the login of a user that has such privileges.

Note that if you do not run the task with privileges, the scheduled update will be run with the privileges of the current user account. If no users are currently registered on the computer, running updates under another user account has not been configured, and updates run automatically, they will run with the SYSTEM privileges.

➤ *To start the task with the privileges of a different user account:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, in the **Update settings** section, click the **Configure** button.
5. In the window that will open, on the **Additional** tab, in the **Run mode** section, check the **Run task as** box. Enter the data for the login that you want to start the task as below: user name and password.

RUN MODE: CREATING A SCHEDULE

All virus scan tasks can be started manually, or by a schedule.

When creating a schedule on tasks launch it is necessary to set the interval of the update tasks.

If it is not possible to start the task for any reason (for example, the computer was not on at specified time), you can configure the task to start automatically as soon as it becomes possible.

➤ *To edit a schedule for scan tasks:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, press the **Change** button in the **Run mode** section.
5. Make the required changes in the **Schedule** window that will open.

➤ *To configure automatic launches of skipped tasks:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, press the **Change** button in the **Run mode** section.
5. In the **Schedule** window that will open, in the **Schedule settings** section, check the **Run task if skipped** box.

SELECTING OBJECTS TO UPDATE

Update objects are the components that will be updated:

- application databases;
- application modules.

Application databases are always updated while application modules are only updated if an appropriate mode is selected.

If there is a set of application modules in the update source when updating, Kaspersky Anti-Virus will download and install it when the computer is restarted. Downloaded module updates will not be installed until the computer is restarted.

If the next application update occurs before the computer is restarted and hence before the previously downloaded application module updates are installed, only the threat signatures will be updated.

➔ *If you want to download and install updates for application modules, please do the following:*

1. Open the main application area.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, in the **Update settings** section, check the **Update application modules** box.

CHANGING THE UPDATE TASK'S RUN MODE

You can select the run mode for Kaspersky Anti-Virus update task by using the application configuration wizard (see section "Configuring the update settings" on page [25](#)). You can change the run mode you have selected.

The update task can be launched using one of the following modes:

- **Automatically.** Kaspersky Anti-Virus checks the update source for update packages at specified intervals. If new updates are found, Kaspersky Anti-Virus downloads and installs them on the computer. This is the default mode.

Kaspersky Anti-Virus will attempt to perform updates at intervals specified in the previous update package. This option allows Kaspersky Lab to regulate the updating frequency in case of virus outbreaks and other potentially dangerous situations. Your application will receive the latest updates for the databases, network attacks, and software modules in a timely manner, thus excluding the possibility for malware to penetrate your computer.

- **On schedule** (time interval changes depending on settings). Updates will run automatically according to the schedule created.
- **Manually.** If you select this option, you will run application updates on your own. Kaspersky Anti-Virus will notify you when updates are required without fail.

➔ *To configure the update task launch schedule:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, select the update task launch mode in the **Run mode** section. If the scheduled update option is selected, create the schedule.

UPDATING FROM A LOCAL FOLDER

The procedure of retrieving updates from a local folder is arranged as follows:

1. One of the computers on the network retrieves the Kaspersky Anti-Virus update package from a Kaspersky Lab's server, or from a mirror server hosting the current set of updates. The updates retrieved are placed in a shared folder.
2. Other computers on the network access the shared folder to retrieve updates.

Kaspersky Anti-Virus 6.0 only retrieves its update packages from Kaspersky Lab's servers. We recommend distributing updates for other Kaspersky Lab's applications through Kaspersky Administration Kit.

➤ *To enable update distribution mode, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Additional** tab, in the **Update distribution** section, check the **Copy updates to folder** box and in the field below specify the path to a public folder into which downloaded updates will be copied. Also, you can select the path in the window that will open by clicking the **Browse** button.

➤ *If you wish application updates to be performed from the shared folder selected, please do the following on all computers on the network:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Update source** tab, click the **Add** button.
6. In the **Select update source** window that will open, select a folder or enter the full path to it in the **Source** field.
7. Uncheck the **Kaspersky Lab's update servers** box on the **Update source** tab.

UPDATE STATISTICS

You will find general information on update tasks in the statistics window. In this window, you can also view the events occurred when executing a task (the *Events* tab) and view the list of settings that determine the task execution (the *Settings* tab).

If any errors have occurred during the scan, try running it again. If the next attempt returns an error, we recommend that you save the report on task results in a file using the **Save as** button. Then contact the Technical Support Service, and send the report file. Kaspersky Lab's specialists will certainly help you.

Brief update statistics are displayed in the top part of the statistics window. It includes the size of downloaded and installed updates, update speed and duration, and other information.

➤ *To view statistics of a virus scan task, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section, create an update task, and launch it. The task progress will be displayed in the main window. You can switch the statistics window by clicking the **Details** link.

POSSIBLE PROBLEMS DURING THE UPDATE

When you update Kaspersky Anti-Virus application modules or threat signatures, errors may occur, which is associated with incorrect update configuration, connection problems, etc. This Help section covers the major part of errors and gives

tips for eliminating them. If you encounter errors not covered in Help or want detailed recommendations for eliminating them, try finding information in the Knowledge Base in the Technical Support web portal in the "If a program generated an error..." section. If recommendations given in this section are not helpful in solving the problem or if there is no information about the error in the Knowledge Base, send a request to the Technical Support Team.

<p>CONFIGURATION ERRORS</p> <p>Errors of this group occur largely due to an incorrect installation of the application, or due to modifications of the application configuration, which resulted in a loss of functionality.</p> <p><u>General recommendations:</u></p> <p>If errors in this group are generated, we recommend restarting updates. If the error persists, contact Technical Support.</p> <p>If the problem is connected to the application being installed incorrectly, we recommend reinstalling it.</p>
<p><i>No update source specified</i></p> <p>None of the source contains update files. It is possible that no update source is specified in the update settings. Please make sure that the update settings are configured correctly and try again.</p>
<p><i>Error verifying license</i></p> <p>This error is generated if the license key used by the application is blocked and placed in the license black list.</p>
<p><i>Error retrieving update settings</i></p> <p>Internal error retrieving update task settings. Please make sure that update settings are configured correctly and try again.</p>
<p><i>Insufficient privileges to update</i></p> <p>This error usually occurs when the user account used to start the update does not have access privileges to the update source. We recommend making sure that user account has the necessary privileges.</p> <p>This error could also be generated when attempt to copy update files to a folder that cannot be created.</p>
<p><i>Internal error</i></p> <p>Internal logical error in update task. Please make sure that the update settings are configured correctly and try again.</p>
<p><i>Error verifying updates</i></p> <p>This error is generated if the files downloaded from the update source do not pass internal verification. Please try updating later.</p>
<p>ERRORS THAT OCCUR WHEN WORKING WITH FILES AND FOLDERS</p> <p>This type of error occurs when the user account being used to run updates has restricted rights or no rights to access the update source or the folder where the updates are located.</p> <p><u>General recommendations:</u></p> <p>If errors of this type occur, we recommend verifying that the user account has sufficient access rights to those files and folders.</p>
<p><i>Cannot create folder</i></p> <p>This error is generated if a folder cannot be created during the update procedure.</p>
<p><i>Insufficient privileges to execute file operation</i></p> <p>This error occurs if the user account used to run the update does not have sufficient privileges to execute operations with the files.</p>
<p><i>File or folder not found</i></p> <p>This error occurs if a file or folder needed in updates is missing. We recommend verifying that the specified file or folder exists and is available.</p>

<p><i>File operation error</i></p> <p>This error is an internal logical error of the update module when executing operations with files.</p>
<p>NETWORK ERRORS</p> <p>Errors of this group occur when there are connection problems or when network connection is not configured correctly.</p> <p><u>General recommendations:</u></p> <p>If errors in this group occur, we recommend making sure your computer is connected to the Internet, the connection settings are correctly configured, and the update source is available. Then try updating again. If the problem persists, contact Technical Support.</p>
<p><i>Network error</i></p> <p>An error was generated while retrieving update files. If you encounter this error, check your computer's network connection.</p>
<p><i>Connection interrupted</i></p> <p>This error occurs when the connection with the update source is terminated by the update server for any reason.</p>
<p><i>Network operation timeout</i></p> <p>Update source connection timeout. When configuring the program's update settings, you may have set a low time-out value for the connection with the update source. If your computer cannot connect to the server or the update folder within that time, the program returns this error. In such a case, we recommend checking that the settings for Updater are correct and that the update source is available.</p>
<p><i>Authorization error on FTP server</i></p> <p>This error occurs if authorization settings for the FTP server used as the update source are entered incorrectly. Please make sure that the actual FTP server settings allow this user account to download files.</p>
<p><i>Authorization error on proxy server</i></p> <p>This error is generated if the settings for updating via a proxy server incorrectly indicate the name and password, or if the user account under which the updates are run does not have access privileges to the update source. Please, edit the authorization settings and retry the update.</p>
<p><i>Error resolving DNS name</i></p> <p>This error is generated if no update source is detected. It is possible that the update source address is indicated incorrectly, the network settings are incorrect, or the DNS server is unavailable. We recommend checking your update settings and availability of update sources, then try again.</p>
<p><i>Connection to the update source could not be established</i></p> <p>This error occurs is there is no connection with the update source. Please make sure that the update source settings are configured correctly and try again.</p>
<p><i>Connection to the proxy server could not be established</i></p> <p>This error is generated if the proxy server connections settings are indicated incorrectly. To solve the problem, we recommend making sure that settings are configured correctly, the proxy server is available, and the Internet is available, and trying to update again.</p>
<p><i>Error resolving proxy server DNS name</i></p> <p>This error is generated if the proxy server is not detected. We recommend making sure that the proxy server settings are correct and that the DNS server is available.</p>

<p>ERRORS RELATED TO CORRUPTED DATABASES</p> <p>These errors are linked to corrupted files in the update source.</p> <p><u>General recommendations:</u></p> <p>If you are updating from Kaspersky Lab web servers, try updating again. If the problem persists, contact Technical Support.</p> <p>If you are updating from a different source, such as a local folder, we recommend updating it from Kaspersky Lab's web servers. If the error occurs again, contact Kaspersky Lab Technical Support.</p>
<p><i>File not in update source</i></p> <p>All files downloaded and installed on your computer during the update process are listed in a special file included in the update. This error occurs if there are any files on the update list that are not on the update source.</p>
<p><i>Error verifying signature</i></p> <p>This error might be returned by the application if the electronic digital signature of the update pack being downloaded is corrupted or does not match the Kaspersky Lab signature.</p>
<p><i>Index file corrupted or missing</i></p> <p>This error is generated if the .xml format index file used for updating is missing from the update source or corrupted.</p>
<p>ERRORS RELATED TO UPDATING USING KASPERSKY ADMINISTRATION KIT ADMINISTRATION SERVER</p> <p>These errors are generated in connection with problems updating the application through Kaspersky Administration Kit Administration Server.</p> <p><u>General recommendations:</u></p> <p>First, make sure that Kaspersky Administration Kit and its components (Administration Server and Network Agent) are installed and running. Try updating again. If this fails, restart Network Agent and Administration Server, then try updating again. If this does not resolve the issue, contact Technical Support.</p>
<p><i>Error connecting to Administration Server</i></p> <p>This error is generated if the Kaspersky Administration Kit Administration Server cannot be connected to. We recommend making sure that NAgent is installed and running.</p>
<p><i>Registration error in NAgent</i></p> <p>If this error occurs, follow the general recommendations for resolving this type of error. If the error reoccurs, send the detailed report file for the update and Network Agent on that computer to Technical Support Service using the online form. Describe the situation in detail.</p>
<p><i>Cannot establish connection. The Administration Server is busy and cannot process the request</i></p> <p>In this case, the update should be attempted later.</p>
<p><i>Cannot establish connection with Administration Server / Main Administration Server / NAgent, physical error / unknown error</i></p> <p>If you encounter such errors, we recommend trying to update again later. If the problem persists, contact Technical Support.</p>
<p><i>Error retrieving file from Administration Server, invalid transport argument</i></p> <p>If the error persists, contact Technical Support.</p>
<p><i>Error retrieving file from Administration Server</i></p> <p>If you encounter such errors, we recommend trying to update again later. If the problem persists, contact Technical Support.</p>

VARIOUS CODES

This group includes errors that cannot be included in any of the groups listed above.

Files for rollback operation missing

This error is generated if another rollback attempt has been made after completing rollback of updates, but no updates had been made between them. The rollback procedure cannot be repeated until a successful update which restores a backup set of files has been performed.

CONFIGURING APPLICATION SETTINGS

The application settings window is used for quick access to the main settings of Kaspersky Anti-Virus 6.0.

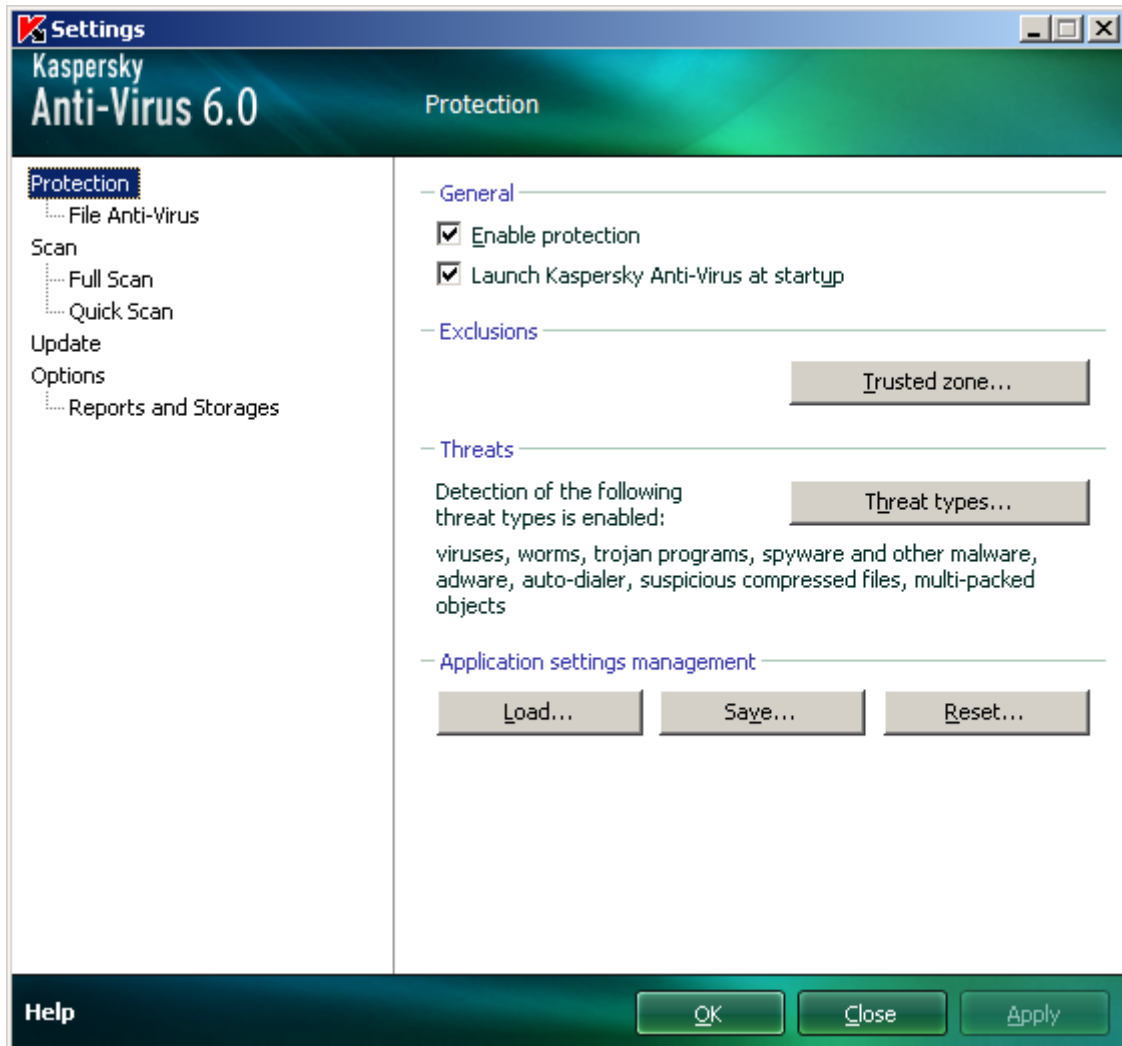


Figure 9. Application settings configuration window

The window consists of two parts:

- the left part of the window provides access to File Anti-Virus components, virus scan tasks, update tasks, etc.;
- the right part of the window contains a list of settings for the component, task, etc., selected in the left part of the window.

You can open this window:

- From the main application window. To do so, click the **Settings** button in the top part of the main window.

- From the context menu. To do so, select the **Settings** item from the application context menu.



Figure 10. Context menu

IN THIS SECTION

Protection	70
File Anti-Virus	76
Scan	77
Update	78
Settings	78
Reports and Storages.....	83

PROTECTION

In the **Protection** window you can use the following additional functions of Kaspersky Anti-Virus:

- Enabling / disabling application protection (see page [71](#)).
- Launching the application at the operation system startup (see page [71](#)).
- Selecting the detectable threat categories (see page [71](#)).
- Creating a trusted zone (see page [72](#)):
 - creating an exclusion rule (see page [72](#));
 - creating a list of trusted applications (see page [74](#));
 - exporting / importing trusted zone components (see page [75](#)).
- Exporting / importing the application settings (see page [75](#)).
- Restoring the default application settings (see page [76](#)).

ENABLING / DISABLING COMPUTER PROTECTION

By default, Kaspersky Anti-Virus is launched when the operating system loads, and protects your computer until it is switched off. File Anti-Virus is running.

You can disable all protection provided by File Anti-Virus.

Kaspersky Lab strongly recommends that you do not disable protection since this could lead to an infection occurrence on your server and data loss.

As a result of disabling protection, File Anti-Virus will be stopped. Disabling component does not affect the execution of virus scan and update tasks of Kaspersky Anti-Virus.

➤ *To disable protection completely:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. Uncheck the **Enable protection** box.

LAUNCHING THE APPLICATION AT THE OPERATING SYSTEM STARTUP

If you have to shut down Kaspersky Anti-Virus completely for any reason, select the **Exit** item from the application's context menu. Then the application will be discarded from RAM. That means that the computer will be running unprotected.

You can enable the computer's protection by starting the application from the **Start** → **Programs** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0** menu.

Protection can also be resumed automatically after restarting your operating system.

➤ *To enable the mode of launching the application at the operating system startup, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. Check the **Launch Kaspersky Anti-Virus at startup** box.

SELECTING DETECTABLE THREAT CATEGORIES

Kaspersky Anti-Virus protects you against various types of malicious programs. Regardless of the settings selected, the application will always scan and disinfect viruses and Trojans. These programs can do significant harm to your computer. To provide more security to your computer, you can enlarge the list of threats to be detected, by enabling the control of various potentially dangerous programs.

➤ *To select the detectable threat categories, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Threats** section, click the **Threat types** button.
4. In the **Threat types** window that will open, check the boxes for the categories of threats you want to protect your computer from.

CREATING A TRUSTED ZONE

Trusted zone is a user-created list of objects that Kaspersky Anti-Virus does not monitor. In other words, it is a set of exclusions from the application's protection scope.

The user creates a trusted zone based on the features of the objects he or she works with, and on the applications installed on the user's computer. You might need to create such an exclusion list if, for example, Kaspersky Anti-Virus blocks access to an object or an application which you are sure is absolutely safe.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or an application), programs' processes, or objects according to the Virus Encyclopedia classification (status assigned to objects by Kaspersky Anti-Virus during a scan).

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

➔ *To create the list of exclusions from scan, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Exclusions** section, click the **Trusted zone** button.
4. In the window that will open, configure exclusion rules for objects (see page [72](#)), and create the list of trusted applications (see page [74](#)).

SEE ALSO

Creating an exclusion rule	72
Allowed file exclusion masks	73
Allowed exclusion masks according to the Virus Encyclopedia	74
Creating the list of trusted applications	74
Exporting / importing trusted zone components	75

CREATING AN EXCLUSION RULE

Exclusion rules are sets of conditions that Kaspersky Anti-Virus uses to verify if it can skip the scan of an object.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or an application), program processes, or objects according to the Virus Encyclopedia's classification.

Threat type is the status Kaspersky Anti-Virus assigns to an object while scanning it. This status is assigned based on the classification of malware and riskware found in the Kaspersky Lab's Virus Encyclopedia.

Potentially dangerous software does not have malicious functions but it can be used as an auxiliary component for a malicious code, since it contains holes and errors. This category includes, for example, remote administration applications, IRC clients, FTP servers, all-purpose utilities for halting or hiding processes, keyloggers, password macros, autodialers, etc. Such software is classified as not-a-virus, but it can be divided into several types, e.g. Adware, Joke, Riskware, etc. (for more information on potentially dangerous software detected by Kaspersky Anti-Virus, see the Virus Encyclopedia at www.viruslist.com (<http://www.viruslist.com/en/viruses/encyclopedia>)). After the scan, such programs may be blocked. Since many of them are widely exploited by users, they may be excluded from the scan. To do so, you should add the name of the threat or a threat name mask (according to the Virus Encyclopedia's classification) to the trusted zone.

For example, you may frequently use the Remote Administrator program. This is a remote access system that allows you to operate your resources from a remote computer. Kaspersky Anti-Virus views this sort of application activity as potentially dangerous and may block it. To avoid blocking the application, you should create an exclusion rule that would specify Remote Admin as the verdict.

When an exclusion is being added, it results in a rule, which further can be used by File Anti-Virus, and at the execution of virus scan tasks .

➡ *To create an exclusion rule, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Exclusions** section, click the **Trusted zone** button.
4. In the window that will open, on the **Exclusion rules** tab, click the **Add** button.
5. In the **Exclusion mask** window that will open, in the **Properties** section, select an exclusion type. Then, in the **Rule description** section, assign values to the selected exclusion types and select which Kaspersky Anti-Virus components should be covered by the rule.

➡ *To create an exclusion rule from the report window, please do the following:*

1. Select the object from the report to add to the exclusions.
2. Select the **Add to Trusted zone** item from the context menu for this object.
3. In the **Exclusion mask** window that will open, make sure that you are satisfied with the exclusion rule settings. Object name and relevant threat type fields are filled in automatically based on report data. To create the rule, click the **OK** button.

ALLOWED FILE EXCLUSION MASKS

Let us take a closer look at some examples of allowed masks that you can use when creating the list of files to exclude from scan:

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

If you do not want the application to scan files in all nested subfolders of the specified folder, check the **Include subfolders** box when creating the mask.

3. File path masks:
 - **dir*.***, or **dir***, or **dir** – all files in all dir\ folders;

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

If you do not want the application to scan files in all nested subfolders of the specified folder, check the **Include subfolders** box when creating the mask.

The ****** and ***** exclusion masks can only be used if you specify the classification type of the threat according to the Virus Encyclopedia. In this case, the specified threat will not be detected in any object. Using those masks without specifying the classification type essentially disables monitoring. Also, when setting an exclusion, it is not recommended selecting a path related to a network disk created based on a file system folder using the *subst* command, as well as to a disk which mirrors a network folder. The case is that different resources may be given the same disk name for different users, which will inevitably lead to an incorrect triggering of exclusion rules.

SEE ALSO

Allowed exclusion masks according to the Virus Encyclopedia [74](#)

ALLOWED EXCLUSION MASKS ACCORDING TO THE VIRUS ENCYCLOPEDIA

When adding masks to exclude certain threats based on their Virus Encyclopedia classification, you can specify the following:

- the full name of the threat as given in the Virus Encyclopedia at www.viruslist.com (<http://www.viruslist.com>), e.g. **not-a-virus:RiskWare.RemoteAdmin.RA.311** or **Flooder.Win32.Fuxx**;
- the threat name by mask, e.g.:
 - **not-a-virus*** – exclude legal but potentially dangerous programs from scan, as well as joke programs;
 - ***Riskware.*** – exclude riskware from scan;
 - ***RemoteAdmin.*** – exclude all remote administration programs from scan.

SEE ALSO

Allowed file exclusion masks [73](#)

CREATING THE LIST OF TRUSTED APPLICATIONS

You can create a trusted applications list. The activity of such programs, including suspicious activity, file activity, network activity and attempts to access the system registry, will not be monitored.

For example, you may feel that objects used by Microsoft Windows **Notepad** are safe and do not need to be scanned. In other words, you do trust this application. To exclude from scan the objects used by this process, add the **Notepad** application to the list of trusted applications. At the same time, the executable file and the trusted application's process will be scanned for viruses as they were before. To completely exclude an application from the scan, you should use exclusion rules.

Besides, some actions classified as dangerous may be stated as normal by a number of applications. For example, applications that automatically toggle keyboard layouts, such as Punto Switcher, regularly intercept text being entered on your keyboard. To take into account the specifics of such applications and disable the monitoring of their activity, you are advised to add them to the list of trusted applications.

Using trusted application exclusion can also solve potential compatibility conflicts between Kaspersky Anti-Virus and other applications (for example, network traffic from another computer that has already been scanned by the anti-virus application) and can boost computer productivity, which is especially important when using server applications.

By default, Kaspersky Anti-Virus scans objects being opened, run, or saved by any program process, and monitors the activity of all applications and the network traffic they create.

➤ *To add an application to the trusted list, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Exclusions** section, click the **Trusted zone** button.
4. In the window that will open, on the **Trusted applications** tab, click the **Add** button.
5. In the **Trusted application** window that will open, select the program by clicking **Browse** button. A context menu will open; by clicking the **Browse** item, you can go to the standard file selection window and select the path to the executable file, or by clicking the **Applications** item, you can switch to the list of currently running applications and select one of them or more, if necessary. Specify settings required for the selected application.

EXPORTING / IMPORTING TRUSTED ZONE COMPONENTS

Using export and import, you can transfer the created exclusion rules and trusted applications lists onto other computers.

➤ *To copy the exclusion rules, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Exclusions** section, click the **Trusted zone** button.
4. In the window that will open, on the **Exclusion rules** tab, use the **Export** and **Import** buttons to perform the required actions to copy the rules.

➤ *To copy the trusted applications list, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Exclusions** section, click the **Trusted zone** button.
4. In the window that will open, on the **Trusted applications** tab, use the **Export** and **Import** buttons to perform the required actions to copy the list.

EXPORTING / IMPORTING KASPERSKY ANTI-VIRUS SETTINGS

Kaspersky Anti-Virus provides the option of importing and exporting its settings.

This is a helpful feature when, for example, the application is installed on your home computer and in your office. You can configure the application the way you want it at home, export those settings as a file on a disk, and load them on your computer at work using the import feature. The settings are stored in a special configuration file.

➤ *To export the application's current settings, please do the following:*

1. Open the application settings window.

2. In the left part of the window, select the **Protection** section.
3. In the **Application settings management** section, click the **Save** button.
4. In the window that will open enter the name of the configuration file and the path where it should be saved.

➔ *To import the application's settings from a saved configuration file, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Application settings management** section, click the **Load** button.
4. In the window that will open, select a file that you wish to import the Kaspersky Anti-Virus settings from.

RESTORING THE DEFAULT SETTINGS

You can always return to the default or recommended settings of Kaspersky Anti-Virus. They are considered optimum, and are recommended by Kaspersky Lab. Application Configuration Wizard restores default settings.

In the window that will open, you will be offered to specify which settings should or should not be saved along with restoration of the required security level.

After you have finished with the Wizard, the **Recommended** security level will be set for File Anti-Virus taking into account the settings that you have decided to keep intact at the restoration. In addition, the settings that you have specified when working with the Wizard will also be applied.

➔ *To restore protection settings, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Application settings management** section, click the **Reset** button.
4. In the window that will open, check the boxes for the settings requiring to be saved. Click the **Next** button. The Initial Configuration Wizard will be launched; follow its directions.

FILE ANTI-VIRUS

The **File Anti-Virus** component settings are grouped in the window (see section "Anti-virus protection of the computer file system" on page [36](#)). By editing the application's settings, you can:

- change the security level (see page [38](#));
- change the action taken on detected objects (see page [38](#));
- create a protection scope (see page [39](#));
- optimize the scan (see page [41](#));
- configure the scan of compound files (see page [41](#));
- change the scan mode (see page [42](#));
- use the heuristic analysis (see page [40](#));
- pause the component (see page [43](#));

- select a scan technology (see page [42](#));
- restore the default protection settings (see page [43](#)) if they have been changed.

➔ *To proceed to the File Anti-Virus settings, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **File Anti-Virus** section.
3. In the right part of the window, select the component settings for security level and reaction to the threat. Click the **Customize** button in order to switch to the other File Anti-Virus settings.

SCAN

Selection of the method to be used to scan objects on your computer is determined by a set of properties assigned for each task.

Kaspersky Lab specialists distinguish several virus scan tasks. They are as follows:

Scan

Scan of objects selected by the user. You can scan any object in the computer's file system.

Full Scan

A thorough scan of the entire system. The following objects are scanned by default: system memory, programs loaded at startup, system backup, email databases, hard drives, removable storage media, and network drives.

Quick Scan

Virus scan of operating system startup objects.

The settings window of each task allows you to do the following:

- select the security level (see page [49](#)) with the settings that the task will use;
- select an action (see page [49](#)) that the application will apply when it detects an infected / potentially infected object;
- create a schedule (see page [55](#)) to run tasks automatically;
- specify the file types (see page [50](#)) to be scanned for viruses;
- specify the scan settings for compound files (see page [52](#));
- select scan methods and scan technologies (see page [52](#));
- assign common scan settings to all tasks (see page [56](#)).

➔ *To edit task settings, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Scan (Full Scan, Quick Scan)** section.
3. In the right part of the window, select the required security level, the reaction to the threat and configure the run mode. Click the **Customize** button in order to switch to the settings of other tasks' settings. To restore the default settings, click the **Default level** button.

UPDATE

Kaspersky Anti-Virus update is performed using settings that determine the following:

- the source (see page [60](#)) from which updates will be downloaded and installed;
- the application update run mode (see page [63](#)) and the specific components to be updated (see page);
- how often the update will be launched if scheduled launch is configured (see page [62](#));
- which account (see page [61](#)) the update will be launched under;
- if the updates are to be copied to a local source (see page [63](#));
- use of a proxy server (see page [61](#)).

➔ *To proceed to update configuration, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Update** section.
3. Select the required run mode in the right part of the window. Click the **Configure** button to switch to configuring other tasks.

OPTIONS

Using the **Options** window you can use the following additional functions of Kaspersky Anti-Virus:

- Application self-defense (see page [78](#)).
- Restricting the access to the application (see page [79](#)).
- Limiting the size of iSwift files (see page [80](#)).
- Server performance when using multiprocessor configuration (see page [80](#)).
- Notifications about Kaspersky Anti-Virus events (see page [81](#)):
 - selecting event type and way of sending notifications (see page [81](#));
 - configuring email notification (see page [82](#));
 - configuring the event log (see page [82](#)).
- Active interface elements (see page [82](#)).

APPLICATION SELF-DEFENSE

Kaspersky Anti-Virus ensures your computer's security against malware and, because of that, can be the target of malicious programs which may try to block or even delete it.

To ensure your computer security system's stability, the application has its own mechanisms of self-defense and protection against remote access.

In Microsoft Windows Server 2008 (without installed Service Packs) and Windows Server 2003 64-bit operating systems, self-defense is only available to prevent Kaspersky Anti-Virus's own files on local drives and system registry records from being modified or deleted.

When protection against remote access is enabled, it is still sometimes required to allow remote administration programs (such as RemoteAdmin) to manage the application. To do so, you should add these programs to the list of trusted applications and enable the **Allow interaction with application interface** setting for them.

➔ *To enable the Kaspersky Anti-Virus's self-defense mechanisms, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Self-Defense** section, check the **Enable Self-Defense** box to deploy the Kaspersky Anti-Virus's protective mechanisms against changes or deletion of its own files on the hard drive, RAM processes, and system registry records.

In the **Self-Defense** section, check the **Disable external control of system service** box to block any attempt to remotely manage the application's services.

If any of the actions listed are attempted, a message will appear over the application icon in the taskbar notification area (unless the notification service has been disabled by the user).

APPLICATION ACCESS RESTRICTION

Your personal computer may be used by several people with varying levels of computer literacy. Leaving open access to Kaspersky Anti-Virus and its settings may dramatically lower the computer's security level as a whole.

To increase the security level of your computer, use a password to access Kaspersky Anti-Virus. This can block all operations, except for notifications of detecting dangerous objects, and prevent the following actions from being performed:

- changing application settings;
- closing the application;
- disabling File Anti-Virus and scan tasks;
- disabling policy (when application is working via Kaspersky Administration Kit);
- removing the application.

Each of the actions listed above leads to a lower level of protection on your computer, so try to establish which of the users on your computer you trust to take such actions.

➔ *To protect access to the application with a password, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Password protection** section, check the **Enable password protection** box and click the **Settings** button.
4. In the **Password protection** window that will open, enter the password and specify the area to be covered by the access restriction. Now whenever any user on your computer attempts to perform the actions you have selected, the application will always request the password.

RESTRICTING THE SIZE OF ISWIFT FILES

iSwift files are files that contain information about NTFS objects already scanned for viruses (iSwift technology). The use of these files allows speeding up the scan as Kaspersky Anti-Virus scans only the objects that have been modified since the last scan. With the time, the size of iSwift files gets large. We recommend that you restrict the size of these files. Once its value is reached, the iSwift-file will be cleared.

➔ *To limit the size of iSwift files, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Resources** section, check the **Reset iSwift database on reaching** box and specify the database size in MB next to it.

MULTIPROCESSOR SERVER CONFIGURATION

When using multiprocessor server configuration, you can manage server performance in the following ways:

- Set the number of copies of the anti-virus kernel to be loaded when Kaspersky Anti-Virus is running on the server (i.e. number of anti-virus processes running on the server in parallel).

The more copies of the anti-virus kernel are running, the faster objects are processed by anti-virus. However, this affects the overall server performance. Failures in File Anti-Virus operation may occur if RAM volume is insufficient or large number of anti-virus kernel copies are running.

In addition, several antivirus processes running on the server simultaneously ensure the continuous server protection in case of a kernel failure.

- Control the server load: for example, reserve one processor section for anti-virus processing of objects, and another section for the server's primal tasks.

Kaspersky Lab recommends reserving at least one processor for server tasks when running on a multiprocessor server.

➔ *To set the number of copies of the anti-virus kernel, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Multi-CPU configuration** section, press the **Details** button.
4. In the **Multi-CPU configuration** window that will open, in the **Parameters** section, specify the number of copies of the anti-virus kernel.

➔ *To balance the server load, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Multi-CPU configuration** section, press the **Details** button.
4. In the **Multi-CPU configuration** window that will open, in the **Utilized processors** section, uncheck the boxes for processors that should be reserved strictly for server operation.

NOTIFICATIONS ABOUT KASPERSKY ANTI-VIRUS EVENTS

Different types of events occur during the operation of Kaspersky Anti-Virus. They may be of reference type or contain important information. For example, an event can inform you of a successful completion of an application update, or can record an error in the operation of a certain component that should be immediately eliminated.

To keep up with the most recent events in Kaspersky Anti-Virus operation, use the notification feature.

Notifications can be delivered in one of the following ways:

- pop-up messages appearing over the application icon in the system tray;
- sound notification;
- email messages;
- recording information in the event log.

➔ *To use the notification service, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Appearance** section, check the **Enable notifications** box and click the **Settings** button.
4. In the **Notification settings** window that will open, specify the types of Kaspersky Anti-Virus events that you want to be notified of, and the types of notification as well.

SEE ALSO

Selecting event type and way of sending notifications	81
Configuring notification by email.....	82
Configuring event log.....	82

SELECTING EVENT TYPE AND WAY OF SENDING NOTIFICATIONS

During Kaspersky Anti-Virus operation, the following kinds of events arise:

- **Critical notifications** are events of critical importance. It is highly recommended that they are reported of with notifications since they point to problems in the application's operation or gaps in your computer's protection. For example, *databases are obsolete* or *license validity period has expired*.
- **Error notifications** are events that lead to the application's inoperability. For example, *databases are missing or corrupted*.
- **Important notifications** are events that should be attended to because they reflect important situations in the application's operation. For example, *databases are obsolete* or *license expires soon*.
- **Minor notifications** are reference-type messages that do not contain important information, as a rule. For example, *object quarantined*.

➔ *To specify which events the application should notify you of and how, please do the following:*

1. Open the application settings window.

2. In the left part of the window, select the **Options** section.
3. In the **Appearance** section, check the **Enable notifications** box and click the **Settings** button.
4. In the **Notification settings** window that will open, check the boxes for the events and the ways of sending notifications for them, which you want to be notified of.

CONFIGURING NOTIFICATION BY EMAIL

After you have selected the events (see section "Selecting event type and way of sending notifications" on page [81](#)) about which you wish to receive a notification by email, you should set up notifications.

➔ *To configure the email notifications, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Appearance** section, check the **Enable notifications** box and click the **Settings** button.
4. In the **Notification Settings** window that will open, check the boxes for the required events in the **Email** field and click the **Email Settings** button.
5. In the **Email notification settings** window that will open, specify the required values for the settings. If you want notifications about events to be sent at scheduled times, create a schedule for sending the information message by clicking the **Change** button. Make the required changes in the **Schedule** window that will open.

CONFIGURING EVENT LOG

Kaspersky Anti-Virus provides the option of recording information about events that occur while the application is running, either in the Microsoft Windows general event log (**Application**) or in a dedicated Kaspersky Anti-Virus event log (**Kaspersky Event Log**).

Logs can be viewed in the Microsoft Windows **Event Viewer** which you can open by using the **Start/Settings/Control Panel/Administration/View Events** option.

➔ *To configure the event log, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Appearance** section, check the **Enable notifications** box and click the **Settings** button.
4. In the **Notification settings** window that will open, check the boxes for the required events in the **Log** field and click the **Log Settings** button.
5. In the **Event Log settings** window that will open, select the log into which the information on events will be recorded.

ACTIVE INTERFACE ELEMENTS

Active interface elements include the following options of Kaspersky Anti-Virus:

Animate taskbar notification area icon.

Depending on the operation being performed by the application, the application icon in the system tray will change. For example, when scanning email messages, a small letter icon appears in front of the application icon. By default,

the application icon is animated. In this case, the icon only displays the protection status of your computer: if the protection is enabled, the icon is in full color; if the protection is paused or disabled, the icon turns grey.

Show "Protected by Kaspersky Lab" on Microsoft Windows logon screen.

By default, this indicator appears in the top right corner of the screen when Kaspersky Anti-Virus starts. It informs you that your computer is protected from any type of threats.

➔ *To configure active interface elements, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. Check the required boxes in the **Appearance** section.

REPORTS AND STORAGES

The section contains the settings that control the operations with application data files.

Application data files are objects that have been quarantined by Kaspersky Anti-Virus, or moved to backup, and files with reports about application components' operation.

In this section, you can:

- configure the report creation and storage (see page [84](#));
- configure quarantine and backup (see page [86](#));
- clear the report archive, Quarantine and Backup.

➔ *To clear the storage areas, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Reports and Storages** section.
3. In the window that will open, click the **Clear** button.
4. In the **Data files** window that will open, specify the storage areas from which all objects should be removed.

SEE ALSO

Principles of handling reports	84
Configuring reports	84
Quarantine for potentially infected objects.....	85
Actions on quarantined objects	85
Backup copies of dangerous objects	86
Working with backup copies	86
Configuring quarantine and backup.....	86

PRINCIPLES OF HANDLING REPORTS

File Anti-Virus operation and the execution of all scan and update tasks are logged in a report.

➤ *To view reports, please do the following:*

1. Open the main application window.
2. Click the **Reports** button.

➤ *To review all the events about component performance or task performance recorded in the report, please do the following:*

1. Open the main application window and click the **Reports** button.
2. In the window that will open, on the **Reports** tab, select the name of a component or a task and click the **Details** link. As a result, a window with detailed information on File Anti-Virus or task operation will open. The resulting statistics on performance are displayed in the upper part of the window, and detailed information is given on the various tabs in the central part. The set of tabs may vary depending on whether the report has been selected for File Anti-Virus or for a task.

➤ *To import the report into a text file, please do the following:*

1. Open the main application window and click the **Reports** button.
2. In the window that will open, on the **Reports** tab, select the name of a component or a task and click the **Details** link.
3. In the window that will open the information about the performance of selected component or task will be shown. Click the **Save As** button and specify where you want to save the report file.

CONFIGURING REPORTS

You can modify the following settings for creating and saving the reports:

- Allow or block logging informative events. As a rule, those events are not critical for the protection (the **Log non-critical events** box).
- Allow the saving in the report only for the events that have occurred since the last startup of the task. This saves disk space by reducing the report size (the **Keep only recent events** box). If the box is checked, the information will be updated every time the task is restarted. However, only non-critical information will be overwritten.
- Set the storage term for reports (the **Store reports no longer than** box). By default, the objects storage time is 30 days; once it expires, the objects will be deleted. You can change the maximum storage time, or even cancel any restrictions imposed on it.
- Specify the maximum report size (the **Maximum size** box). By default, the maximum size is 250 MB. You can cancel any restrictions imposed on the report's size, or enter another value.

➤ *To edit the settings for report creation and storage, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Reports and Storages** section.
3. In the **Reports** section, check all required boxes, and set the storage term and the maximum size of the report, if necessary.

QUARANTINE FOR POTENTIALLY INFECTED OBJECTS

Quarantine is a special repository that stores the objects possibly infected with viruses.

Potentially infected objects are objects suspected of being infected with viruses or their modifications.

Why potentially infected? It is not always possible to exactly determine where an object is infected. This could be for the following reasons:

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

Application databases contain information on the threats investigated to date by Kaspersky Lab's specialists. If a malicious program has been modified and these changes have not been entered into databases yet, Kaspersky Anti-Virus classifies the object infected with the modified malicious program as a potentially infected object, and indicates without fail which threat this infection resembles.

- *The code of the object detected is reminiscent in structure of a malicious program; however, nothing similar is recorded in the application databases.*

It is quite possible that this is a new type of threat, so Kaspersky Anti-Virus classifies that object as a potentially infected object.

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

Potentially infected object may be detected and quarantined when scanning for viruses as well as by File Anti-Virus.

When you place an object to the Quarantine, it is moved, not copied: the object is deleted from the disk or email message, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

SEE ALSO

Actions on quarantined objects [85](#)

Configuring quarantine and backup [86](#)

ACTIONS ON QUARANTINED OBJECTS

You can do the following operations with quarantined objects:

- quarantine the files that you suspect of being infected;
- scan and disinfect all potentially infected objects in Quarantine, using the current application databases;
- restore files to the folders from which they were moved to Quarantine, or to the folders selected by the user;
- delete any quarantined object or a group of selected objects.

► *To take some actions on quarantined objects, please do the following:*

1. Open the main application window and click the **Detected** button.
2. In the window that will open, on the **Quarantine** tab, take the required actions.

BACKUP COPIES OF DANGEROUS OBJECTS

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

Backup copy is a copy of an 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 backup is the ability to restore the original object at any time. Files in backup are saved in a special format and are not dangerous.

SEE ALSO

Working with backup copies	86
Configuring quarantine and backup.....	86

WORKING WITH BACKUP COPIES

You can apply the following operations to the objects stored in backup:

- restore selected copies;
- delete objects.

➔ *To take some actions on backup objects, please do the following:*

1. Open the main application window and click the **Detected** button.
2. In the window that will open, on the **Backup** tab, take the required actions.

CONFIGURING QUARANTINE AND BACKUP

You can edit the following settings for the quarantine and backup:

- Enable the autoscan mode for quarantined objects after each update of the application databases (the **Scan quarantined files after update** box).

Kaspersky Anti-Virus will not be able to scan quarantined objects immediately after updating the application databases if you are working with quarantine.

- Determine the maximum storage time for quarantined objects and for copies of objects in the backup (the **Store objects no longer than** box). By default, the objects storage time is 90 days; once it expires, the objects will be deleted. You can change the maximum storage time, or even cancel any restrictions imposed on it.
- Specify the maximum size of data storage area (the **Maximum size** box). By default, the maximum size is 1000 MB. You can cancel any restrictions imposed on the report's size, or enter another value.

➔ To configure the quarantine and backup settings:

1. Open the application settings window.

2. In the left part of the window, select the **Reports and Storages** section.
3. In the **Quarantine and Backup** section, check the required boxes and specify the maximum size of data storage area, if necessary.

RESCUE DISK

Kaspersky Anti-Virus includes a service allowing the creation of a Rescue Disk.

Rescue Disk is designed to scan and disinfect infected x86-compatible computers. It should be used when the infection is at such level that it is impossible to disinfect the computer using anti-virus applications or malware removal utilities (such as Kaspersky AVPTool) run under the operating system. In this case, a higher degree of efficiency of the disinfection is achieved since malware programs do not gain control when the operating system is being loaded.

Rescue Disk is an .iso file based on the Linux core that comprises the following:

- system files and configuration Linux files;
- a set of operating system diagnostic utilities;
- a set of additional tools (file manager, etc.);
- Kaspersky Rescue Disk files;
- files containing the application databases.

Booting a computer under a corrupted operating system may be achieved in one of the two following ways:

- *locally*, from a CD/DVD. To do so, the computer should be equipped with suitable device.
- *remotely*, from the administrator's workstation or from another computer on the network.

Remote startup is only possible if the computer being booted supports Intel® vPro™ or Intel® Active Management technology.

➔ To create a Rescue Disk, please do the following:

1. Open the main application window.
2. Click the **Rescue Disk** button to run the Rescue Disk Creation Wizard (see page [88](#)).
3. Follow the Wizard instructions.
4. Using the file provided by the wizard, create a boot CD/DVD. To do so, you can use any CD/DVD burning application, such as Nero.

SEE ALSO

Creating the Rescue Disk.....	88
Booting the computer using the Rescue Disk.....	89

CREATING THE RESCUE DISK

Rescue Disk creation means the creation of the disk image (ISO file) with up-to-date application databases and configuration files.

The source disk image serving as base for new file creation can be downloaded from Kaspersky Lab server or copied from a local source.

The image file created by the wizard will be saved in the "*Documents and Settings\All Users\Application Data\Kaspersky Lab\VP80\Data\Rdisk1*" folder (or "*ProgramData\Kaspersky Lab\VP80\Data\Rdisk1*" – for Microsoft Vista) named as *rescuecd.iso*. If the wizard has detected an ISO file created earlier in the specified folder, you can use it as original disk image by checking the **Use existing image** box, and jump to Step 3 – image update (see page [88](#)). If the wizard has not detected any image file, this box is not available.

Rescue Disk is created with a wizard that consists of a series of boxes (steps). The boxes are browsed with the **Back** and **Next**; wizard finishes its activity by clicking the **Finish** button. To stop the wizard at any step, use the **Cancel** button.

DETAILED DISCUSSION OF THE WIZARD STEPS

Step 1. Selecting the disk image source.....	88
Step 2. Copying ISO image	88
Step 3. ISO image update	88
Step 4. Remote startup.....	89
Step 5. Closing the Wizard	89

STEP 1. SELECTING THE DISK IMAGE SOURCE

If you have checked the **Use existing ISO file** box in the previous wizard window, then this step will be skipped.

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

- Select **Copy ISO image from CD/DVD disk or local network** if you already have a Rescue Disk on CD/DVD or an image prepared for it and stored on your computer or on a local network resource.
- Select the **Download ISO image from Kaspersky Lab server** option if you do not have any existing image file, you can download it from a Kaspersky Lab's server (file size is about 100 MB).

STEP 2. COPYING ISO IMAGE

If you have selected the option of copying the image from a local source at the previous step (**Copy ISO image from CD/DVD disk or local network**), then you should specify the path to it at this current step. To do so, use the **Browse** button. Then, the progress of copying will be displayed.

If you have selected **Download ISO image from Kaspersky Lab server**, then the progress of file downloading will be displayed immediately.

STEP 3. ISO IMAGE UPDATE

File update procedure includes:

- update of application databases;
- update of configuration files.

Configuration files determine how the Rescue Disk should be used: on a local computer or on a remote one; thus you should select an option before updating the ISO file:

- **Remote startup** if loading a remote computer is intended.

Note that if booting a remote computer is selected, it should support Intel® vPro™ or Intel® Active Management technology.

If Internet access from a remote computer is ensured by a proxy server, then the update will not be available when using the Rescue Disk. In this case, it is recommended to update Kaspersky Anti-Virus beforehand.

- **Startup from CD/DVD disk** if the disk image being created is intended to record on a CD/DVD.

Having selected the required option, click the **Next** button. The progress of updating is displayed in the next wizard window.

If you have selected the **Remote startup** option, then the created image can be used neither for burning a CD/DVD, nor for loading the computer. To load the computer from a CD/DVD, you should launch the wizard again and select the **Startup from CD/DVD disk** option at that step.

STEP 4. REMOTE STARTUP

This Wizard's step only appears if you have selected the **Remote startup** option at the previous step.

Enter the information about the computer:

- **IP address or computer name** on the network;
- data of user account with system administrator rights: **User name** and **Password**.

The next wizard window is an iAMT console where you can control the computer loading process (see page [89](#)).

STEP 5. CLOSING THE WIZARD

This Wizard window informs you that you have successfully created a Rescue Disk.

BOOTING THE COMPUTER USING THE RESCUE DISK

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

You will need the boot disk image file (.iso) to load the operating system. You can download (see page [88](#)) the file from a Kaspersky Lab's server or update (see page [88](#)) the existing one.

Let us take a closer look at the Rescue Disk functioning. When loading the disk, the following operations are under way:

1. Automatic detection of the computer's hardware.
2. Searching file systems on hard drives. File systems detected will be assigned names starting with C.

Names assigned to hard drives and removable devices may not match names assigned to them by the operating system.

If the operating system of the computer being loaded is in sleeping mode, or its file system has the *unclean* status due to an incorrect shutdown, you will be offered to choose whether you wish to mount the file system or restart the computer.

File system mounting may result in its corruption.

3. Searching the Microsoft Windows swap file *pagefile.sys*. If it is missing, the volume of the virtual memory is limited by the size of the RAM.
4. Selecting the localization language. If the selection has not been done after a lapse of time, then the English language will be set by default.

When loading a remote computer, this step is skipped.

5. Searching (creating) the folders for anti-virus databases, reports, quarantine storage, and additional files. By default the folders of Kaspersky Lab's application installed on the infected computer (*ProgramData/Kaspersky Lab/AVP8* - for Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* - for earlier versions of Microsoft Windows) will be used. If such application folders cannot be found, an attempt to create them will be made. If those folders have not been found, and they cannot be created, the *kl.files* folder will be created on a system disk.
6. Trying to configure network connections based on data found in system files of the computer being loaded.
7. Loading graphical subsystem and starting Kaspersky Rescue Disk (when loading the computer from a CD/DVD).

If a remote computer is loaded in the iAMT console, the command prompt will be loaded. You can use the commands for working with Kaspersky Rescue Disk from the command line to manage tasks (see page [91](#)).


In system rescue mode only virus scan tasks and database updates from a local source are available, as well as update rollback and viewing of statistics.

➡ *To load the operating system of an infected computer from a CD/DVD, please do the following:*

1. In BIOS settings enable booting from CD/DVD-ROM (for detailed information please refer to the documentation for the motherboard installed on your computer).
2. Insert the CD/DVD with Rescue Disk image into the CD/DVD drive of an infected computer.
3. Restart your computer.
4. Further the boot continues according with the algorithm described above.

➡ *To load the operating system of a remote computer, please do the following:*

1. Open the main application window.
2. Click the **Rescue Disk** button to run the Rescue Disk Creation Wizard (see page [88](#)). Follow the Wizard instructions.

Note that you should select the  **Remote startup** option at the disk image update stage (see page [88](#)).

Further the boot continues according with the algorithm described above.

WORKING WITH KASPERSKY RESCUE DISK FROM THE COMMAND PROMPT

You can work with Kaspersky Rescue Disk from the command prompt. Capability is provided to perform the following operations:

- scan selected objects;
- update databases and application modules;
- rolling back the last update
- call up help on command line syntax;
- call up help on command syntax.

Command line syntax:

```
<command> [settings]
```

The following may be used as commands:

HELP	help with command syntax and list of commands
SCAN	scan objects for viruses
UPDATE	update task start
ROLLBACK	last update rollback
EXIT	exit Kaspersky Rescue Disk

IN THIS SECTION

Virus scan.....	91
Kaspersky Anti-Virus update	93
Rolling back the last update	93
Viewing Help	93

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>]
```

Settings description:

<object to scan> – this parameter gives the list of objects that will be scanned for malicious code.

The parameter may include several space-separated values from the list provided.

<files>	<p>List of paths to the files and/or folders to be scanned.</p> <p>You can enter an absolute or relative path to the file. Items on the list are separated by a space.</p> <p>Comments:</p> <ul style="list-style-type: none"> • if the name of the object contains a space, it should be supplied with quotation marks; • if reference is made to a specific directory, all files in the directory are scanned.
/discs/	Scanning all drives.
/discs/<disc_name>:/<folder>	Scanning the selected drive, where <disc_name> is the name of the drive, and <folder> is the path to the folder being scanned.
<p><action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for -i8.</p>	
-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) (this is the default setting).
-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.
<p><file types> – this parameter defines the file types that will be subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents will be scanned.</p>	
-fe	Scan only infected files by extension.
-fi	Scan only infected files by contents.
-fa	Scan all files.
<p><exclusions> – this parameter defines objects that are excluded from the scan.</p> <p>The parameter may include several space-separated values from the list provided.</p>	
-e:a	Do not scan archives.
-e:b	Do not scan email databases.
-e:m	Do not scan plain text emails.
-e:<filemask>	Do not scan objects, which match the mask.

-e:<seconds>	Skip objects that are scanned for longer than the time specified in the <seconds> parameter.
-es:<size>	Skip objects of size (in MB) exceeding the value specified in the <size> parameter.

Examples:

- ▶ *Start scan of the Documents and Settings folder and the <D> drive:*

```
SCAN /discs/D: "/discs/C:/Documents and Settings"
```

KASPERSKY ANTI-VIRUS UPDATE

The command for updating Kaspersky Anti-Virus's databases and program modules features the following syntax:

```
UPDATE [<update_source>] [-R[A]:<report_file>]
```

Settings description:

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

Examples:

- ▶ *Update databases and record all events in a report:*

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
ROLLBACK [-R[A]:<report_file>]
```

Settings description:

-R[A]:<report_file>	<p>-R:<report_file> – log only important events in the report.</p> <p>-RA:<report_file> – log all events in the report.</p> <p>An absolute path to the file is allowed to use. If the parameter is not defined, scan results are displayed on screen, and all events are shown.</p>
----------------------------------	---

Example:

```
ROLLBACK -RA:/discs/C:/rollback.txt
```

VIEWING HELP

Use this command to view the 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>

VALIDATING KASPERSKY ANTI-VIRUS SETTINGS

After Kaspersky Anti-Virus has been installed and configured, you can verify whether the application is configured correctly, using a test "virus" and its modifications. A separate test is required for each protection component / protocol.

IN THIS SECTION

Test "virus" EICAR and its modifications	95
Validating File Anti-Virus settings	96
Validating virus scan task settings	97

TEST "VIRUS" EICAR AND ITS MODIFICATIONS

This test "virus" was specially developed by  (The European Institute for Computer Antivirus Research) for the testing of anti-virus products.

The test "virus" IS NOT A VIRUS, because it does not contain code that can harm your computer. However, most anti-virus products identify this file as a virus.

Never use real viruses for testing the operation of an anti-virus product!

You can download this test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

Before you download the file, you must disable the computer's anti-virus protection, because otherwise the application would identify and process the file *anti_virus_test_file.htm* as an infected object transferred via the HTTP protocol. Do not forget to enable the anti-virus protection immediately after you download the test "virus".

The application identifies the file downloaded from the **EICAR** site as an infected object containing a virus that **cannot be disinfected** and performs the actions specified for this type of object.

You can also modify the standard test "virus" to verify the operation of the application. To modify the "virus", change the content of the standard "virus" by adding one of the prefixes to it (see table below). To modify test "virus", you can use any text or hypertext editor, such as **Microsoft Notepad**, **UltraEdit32**, etc.

You can test the correctness of the operation of the anti-virus application using the modified EICAR "virus" only if your anti-virus bases were last updated on or after October 24, 2003 (October, 2003 cumulative updates).

In the table below, the first column contains the prefixes that must be added at the start of the standard test "virus" string. The second column lists all possible statuses that the Anti-Virus application can assign to the object, based on the results of the scan. The third column indicates how the application processes objects with the specified status. Please note that that actual actions performed on the objects are determined by the application's settings.

After you have added a prefix to the test "virus", save the new file under a different name, for example: *ecar_dele.com*. Assign similar names to all modified "viruses".

Table 1. Modifications of the test "virus"

Prefix	Object status	Object processing information
No prefix, standard test "virus".	Infected. Object contains code of a known virus. You cannot disinfect the object.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed will be that specified for non-disinfectable objects.
CORR-	Corrupted.	The application could access the object but could not scan it because it is corrupted (for example, the file structure is corrupted, or the file format is invalid). You can find the information that the object has been processed in the report on application operation.
WARN-	Suspicious. Object contains code of an unknown virus. You cannot disinfect the object.	The object has been found suspicious by the heuristic code analyzer. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
SUSP-	Suspicious. Object contains modified code of a known virus. You cannot disinfect the object.	The application detected a partial correspondence of a section of object code with a section of code of a known virus. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
ERRO-	Scanning error.	An error occurred during a scan of an object. The application could not access the object, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is scanned on a network resource). You can find the information that the object has been processed in the report on application operation.
CURE-	Infected. Object contains code of a known virus. Disinfectable.	Object contains a virus that can be disinfectable. The application will disinfect the object; the text of the "virus" body will be replaced with the word CURE. You will be notified when an object of this type is detected.
DELE-	Infected. Object contains code of a known virus. You cannot disinfect the object.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed will be that specified for non-disinfectable objects. You will be notified when an object of this type is detected.

VALIDATING FILE ANTI-VIRUS SETTINGS

➤ To verify the correctness of File Anti-Virus configuration, please do the following:

1. Create a folder on a disk, copy into it the test "virus" downloaded from the official **EICAR's** website at (http://www.eicar.org/anti_virus_test_file.htm), and its modifications you have created.
2. Allow all events to be logged so the report file retains data on corrupted objects or objects skipped due to errors.
3. Run the test "virus" or one of its modified versions.

The File Anti-Virus will intercept the call to execute the file, scan it, and perform the action specified in the settings for objects of that status. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

➤ *In order to verify that the virus scan task is correctly configured:*

1. Create a folder on a disk, copy into it the test "virus" downloaded from the official **EICAR**'s website at (http://www.eicar.org/anti_virus_test_file.htm), and its modifications you have created.
2. Create a new virus scan task and select the folder, containing the set of test "viruses", as the object to scan.
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.
4. Run the virus scan task.

When the scan task is running, the actions specified in the task settings will be performed as suspicious or infected objects are detected. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view all information about the virus scan task actions in the report on the component's operation.

TYPES OF NOTIFICATIONS

When Kaspersky Anti-Virus events occur, special notification messages are displayed. Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alarm.** A critical event has occurred, for instance, a malicious object or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. This type of notification is color-coded in red.
- **Warning.** A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide how dangerous you think this event is. This type of notification is color-coded in yellow.
- **Info.** This notification gives information about non-critical events. Informational notifications are color coded in blue.

IN THIS SECTION

Malicious object detected	98
Object cannot be disinfected	99
Suspicious object detected.....	99

MALICIOUS OBJECT DETECTED

If File Anti-Virus or a virus scan detects malicious code, a special notification will pop up.

The notification contains:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Disinfect** – attempt to disinfect the malicious object. Before treatment, a backup copy is made of the object in case the necessity arises to restore it or a portrait of its infection.
- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but take no actions on it; simply record information about it in a report.

You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan task until it is complete.

OBJECT CANNOT BE DISINFECTED

There are some cases when it is impossible to disinfect a malicious object. This could happen if a file is so damaged that it is impossible to delete malicious code from it and restore integrity. The treatment procedure cannot be applied to several types of dangerous objects, such as Trojans.

In such cases, a special notification will pop up containing:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but take no actions on it; simply record information about it in a report.

You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan task until it is complete.

SUSPICIOUS OBJECT DETECTED

If File Anti-Virus or a virus scan detects an object containing code from an unknown virus or modified code of a known virus, a special notification will pop up.

The notification contains:

- The threat type (for instance, *virus*, *Trojan*) and the name of the object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the object and a path to it.

You are asked to select one of the following responses to the object:

- **Quarantine** – place the object to quarantine. When you place an object to the Quarantine, it is moved, not copied: the object is deleted from the disk or email message, and saved in the Quarantine folder. Files in Quarantine are saved in a special format and are not dangerous.

When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the not *infected* status, and then restored.

- **Delete** – delete the object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but perform no actions on it; simply record information about it in a report.

You can later come back to skipped objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan task until it is complete.

If you are sure that the object detected is not malicious, we recommend adding it to the trusted zone to avoid the application making repeat false positives when you use the object.

WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Anti-Virus from the command line.

Command line syntax:

```
avp.com <command> [options]
```

You must access the application from the command line from the Kaspersky Anti-Virus installation folder, or by specifying the full path to avp.com.

The following commands can be used as a <command>:

- **HELP** – help with command syntax and list of commands.
- **SCAN** – scanning of objects for malware.
- **UPDATE** – starts the application update.
- **ROLLBACK** – rolls back to the last Kaspersky Anti-Virus update made (the command can only be executed if the password assigned via the application interface is entered).
- **START** – starts a component or a task.
- **STOP** – stops a component or a task (the command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered).
- **STATUS** – displays the current component or task status on screen.
- **STATISTICS** – displays statistics for the component or task on screen.
- **EXPORT** – exports application protection settings.
- **IMPORT** – imports application protection settings (the command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered).
- **ACTIVATE** – activates Kaspersky Anti-Virus via Internet using an activation code.
- **ADDKEY** – activates the application using a key file (the command can only be executed if the password assigned via the application interface is entered).
- **RESTORE** – restores a file from quarantine.
- **EXIT** – closes the application (the command can only be executed if the password assigned via the application interface is entered).
- **TRACE** – obtains a trace file.

Each command requires its own specific set of parameters.

IN THIS SECTION

Viewing Help	102
Virus scan.....	102
Updating the application.....	104
Rolling back the last update	105
Starting / stopping File Anti-Virus operation or a task.....	105
Statistics on a component's operation or a task	106
Exporting protection settings	107
Importing protection settings	107
Activating the application.....	107
Restoring a file from quarantine	108
Closing the application	108
Obtaining a trace file.....	108
Return codes of the command line.....	109

VIEWING HELP

Use this command to view the application command line syntax:

```
avp.com [ /? | HELP ]
```

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

```
avp.com <command> /?
avp.com HELP <command>
```

VIRUS SCAN

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

```
avp.com SCAN [<object scanned>] [<action>] [<file types>] [<exclusions>] [<report settings>] [<advanced settings>]
```

To scan objects, you can also use the tasks created in the application by starting the one you need from the command line. The task will be run with the settings specified in Kaspersky Anti-Virus interface.

Settings description:

<object to scan> – this parameter gives the list of objects that will be scanned for malicious code. The parameter may include several space-separated values from the list provided:

- **<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. Comments:
 - if the object name contains a space, it must be placed in quotation marks;
 - if reference is made to a specific folder, all files in this folder are scanned.
- **/ALL** – full computer scan.
- **/MEMORY** – RAM objects.
- **/STARTUP** – startup objects.
- **/MAIL** – mail databases.
- **/REMDRIVES** – all removable drives.
- **/FIXDRIVES** – all local drives.
- **/NETDRIVES** – all network drives.
- **/QUARANTINE** – quarantined objects.
- **/@:<filelist.lst>** – path to a file containing a list of objects and catalogs to be scanned. The file should be in text format and each scan object must be listed on a separate line. You can enter an absolute or relative path to the file. The path must be placed in quotation marks even if it contains a space.

<action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for **/i2**. The following values are possible:

- **/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). This is the default setting.
- **/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.

<file types> – this parameter defines the file types that will be subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents will be scanned. The following values are possible:

- **/fe** – scan only infected files by extension.
- **/fi** – scan only infected files by contents.
- **/fa** – scan all files.

<exclusions> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.

- **/e:a** – do not scan archives.
- **/e:b** – do not scan email databases.
- **/e:m** – do not scan plain text emails.
- **/e:<mask>** – do not scan objects, which match the mask.
- **/e:<seconds>** – skip objects that are scanned for longer than the time specified in the **<seconds>** parameter.

<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file.

<advanced settings> – settings that define the use of anti-virus scanning technologies and of the settings configuration file:

- **/iChecker=<on|off>** – enable / disable the use of iChecker technology.
- **/iSwift=<on|off>** – enable / disable the use of iSwift technology.
- **/C:<configuration_file_name>** – defines the path to the configuration file that contains the application settings for the scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

Examples:

- *Start a scan of memory, startup objects, mail databases, the directories My Documents and Program Files and the file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Scan the objects listed in the file object2scan.txt, using the configuration file scan_setting.txt for the job. Use the scan_setting.txt configuration file. When the scan is complete, create a report to log all events:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

A sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

UPDATING THE APPLICATION

The syntax for updating the modules of Kaspersky Anti-Virus and application databases from the command line is as follows:

```
avp.com UPDATE [<update_source>] [/APP=<on|off>] [<report_settings>]
[<advanced_settings>]
```

Settings description:

<update_source> – HTTP or FTP server or network folder for downloading updates. If a path is not selected, the update source will be taken from the application update settings.

/APP=<on|off> – enable / disable application modules update.

<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown. The following values are possible:

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file.

<advanced settings> – settings that define the use of the settings configuration file.

/C:<configuration_file_name> – defines the path to the configuration file that contains the application settings for the scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

Examples:

➤ *Update application databases and record all events in a report:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➤ *Update the Kaspersky Anti-Virus application modules using the parameters of updateapp.ini configuration file:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
avp.com ROLLBACK </password=<password>> [<report_settings>]
```

Settings description:

</password=<password>> – a password assigned via the application interface. The ROLLBACK command will not be executed without entering the password.

<report settings> – settings that define the format of the report on scan results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

Example:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

STARTING / STOPPING FILE ANTI-VIRUS OPERATION OR A TASK

The START command syntax:

```
avp.com START <profile|task_name> [report_settings]
```

The STOP command syntax:

```
avp.com STOP <profile|task_name> </password=<password>>
```

Settings description:

</password=<password>> – a password assigned via the application interface. The STOP command will not be executed without entering the password.

<report settings> – this parameter determines the format of the report on scan results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown. The following values are possible:

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

The **<profile|task_name>** setting can have one of the following values:

- **Protection (RTP)** – all protection components;
- **File_Monitoring (FM)** – File Anti-Virus;
- **Scan_My_Computer** – full computer scan task;
- **Scan_Objects** – objects scan;
- **Scan_Quarantine** – quarantine scan;
- **Scan_Startup (STARTUP)** – startup objects scan;
- **Updater** – update task;
- **Rollback** – updates rollback task.

Components and tasks started from the command line are run with the settings modified through the application's interface.

Examples:

➤ *To enable File Anti-Virus, type the following in the command prompt:*

```
avp.com START FM
```

➤ *To stop the full scan task from the command prompt, enter the following:*

```
avp.com STOP SCAN_MY_COMPUTER /password=<your_password>
```

STATISTICS ON A COMPONENT'S OPERATION OR A TASK

The STATUS command syntax:

```
avp.com STATUS <profile|task_name>
```

The STATISTICS command syntax:

```
avp.com STATISTICS <profile|task_name>
```

Settings description:

The **<profile|task_name>** setting can have one of the values specified in the START / STOP command (see page [105](#)).

EXPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com EXPORT <profile|task_name> <file_name>
```

Settings description:

The **<profile|task_name>** setting can have one of the values specified in the START / STOP command (see page [105](#)).

<file_name> – path to the file to which the application settings are being exported. An absolute or a relative path may be specified.

Example:

```
avp.com EXPORT RTP RTP_settings.dat - binary format
avp.com EXPORT FM FM_settings.txt - text format
```

IMPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com IMPORT <file_name> </password=<your_password>>
```

Settings description:

<file_name> – path to the file from which the application settings are being imported. An absolute or a relative path may be specified.

</password=<your_password>> – a password assigned via the application interface.

Example:

```
avp.com IMPORT settings.dat
```

ACTIVATING THE APPLICATION

You can activate Kaspersky Anti-Virus in two ways:

- via the Internet using an activation code (the ACTIVATE command);
- using a key file (the ADDKEY command).

Command syntax:

```
avp.com ACTIVATE <activation_code> </password=<password>>
avp.com ADDKEY <file_name> </password=<password>>
```

Settings description:

<activation_code> – the activation code: xxxxx-xxxxx-xxxxx-xxxxx.

<file_name> – application key file with the .key: xxxxxxxx.key extension.

</password=<password>> – a password assigned via the application interface.

Example:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
```

```
avp.com ADDKEY 1AA111A1.key </password=<password>>
```

RESTORING A FILE FROM QUARANTINE

Command syntax:

```
avp.com RESTORE [/REPLACE] <file_name>
```

Settings description:

/REPLACE – replacement of existing file.

<file_name> – the name of file to restore.

Example:

```
avp.com REPLACE C:\eicar.com
```

CLOSING THE APPLICATION

Command syntax:

```
avp.com EXIT </password=<password>>
```

Settings description:

</password=<password>> – a password assigned via the application interface. The command will not be executed without entering the password.

OBTAINING A TRACE FILE

You might need to create a trace file if you have problems with Kaspersky Anti-Virus. Trace files are useful to troubleshoot problems, and are extensively used by the specialists at Technical Support.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Settings description:

[on|off] – enable / disable trace file creation.

[file] – output trace to file.

<trace_level> – this value can be an integer from 100 (minimum level, only critical messages) to 600 (maximum level, all messages).

When contacting the Technical Support Service, you should specify the required trace level. If the level is not specified, we recommend setting the value to 500.

Examples:

➔ *To disable trace file creation:*

```
avp.com TRACE file off
```

➔ *Create a trace file with the trace level of 500:*

```
avp.com TRACE file on 500
```

RETURN CODES OF THE COMMAND LINE

The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a specific type of task.

General return codes:

- 0 – operation completed successfully;
- 1 – invalid setting value;
- 2 – unknown error;
- 3 – task completion error;
- 4 – task cancelled.

Virus scan task return codes:

- 101 – all dangerous objects processed;
- 102 – dangerous objects detected.

MODIFYING, REPAIRING, OR REMOVING THE APPLICATION

You can uninstall the application in the following ways:

- using the application setup wizard;
- from the command prompt (see section "Uninstalling the application from the command prompt" on page [111](#));
- using Kaspersky Administration Kit (please refer to Kaspersky Administration Kit Deployment Guide);
- using Microsoft Windows Server 2000/2003 domain group policies (see section "Uninstalling the application" on page [21](#)).

IN THIS SECTION

Modifying, repairing, and removing the application using the Installation Wizard [110](#)

Removing the application from the command prompt [111](#)

MODIFYING, REPAIRING, AND REMOVING THE APPLICATION USING THE INSTALLATION WIZARD

You may find it necessary to repair the application if you have detected errors in its operation after an incorrect configuration or a file corruption.

➤ *To repair or modify missing Kaspersky Anti-Virus components or uninstall the application, please do the following:*

1. Insert the installation CD into your CD/DVD-ROM drive if you have used one to install the application. If you have installed Kaspersky Anti-Virus from a different source (public access folder, folder on your hard drive, etc.), make sure that the application installation package is at the given location and that you have access to it.
2. Select **Start** → **Programs** → **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** → **Modify, Repair, or Remove**.

The installation wizard will then open for the program. Let us take a closer look at the steps of repairing, modifying, or removing the application.

STEP 1. INSTALLATION WELCOME WINDOW

If you have taken all the steps described above and required to repair or modify the application, Kaspersky Anti-Virus installation welcome window will appear. Click the **Next** button to continue.

STEP 2. SELECTING AN OPERATION

At this step, you should select which operation you want to run on the application. You can modify the application components, repair the components that are already installed, or remove several components or the entire application. To execute the operation you need, click the appropriate button. The installation program's response depends on the operation you have selected.

Modifying the application is similar to custom application installation where you can specify which components you want to install, and which you want to delete.

Repairing the application depends on the application components installed. The files will be repaired for all components that have been installed and the **Recommended** security level will be set for each of them.

When Kaspersky Anti-Virus 6.0 is uninstalled remotely, the server will not be rebooted automatically. However, to remove the application components and ensure a proper functioning of the computer in the future, it is recommended to reboot the server manually.

When removing the application, you can select what data created and used by the application you wish to save on your computer. To delete all Kaspersky Anti-Virus data, select the **Complete uninstall** option. To save data, select the **Save application objects** option and specify which objects should not be deleted:

- *Activation information* – key file needed to work with the application.
- *Application databases* - complete set of signatures of dangerous programs, viruses, and other threats current as of the last update.
- *Backup objects* - backup copies of deleted or disinfected objects. We recommend saving these objects, so that they could be restored later.
- *Quarantine objects* - objects that are potentially infected by viruses or modifications of them. These objects contain code that is similar to code of a known virus but it is difficult to determine if they are malicious. It is recommended to save them, since they might prove harmless or could be disinfected after the threat signatures are updated.
- *Protection settings* – values for the settings of all the application components.
- *iSwift data* - database with information on objects scanned in NTFS. This allows increasing scan speed. Using this database, Kaspersky Anti-Virus only scans the files that have been modified since the last scan.

If a long period of time elapses between uninstalling one version of Kaspersky Anti-Virus and installing another, we do not recommend using the iSwift database saved from a previous installation of the application. A malicious program could penetrate the computer during this period and its effects would not be detected by the database, which could lead to an infection.

To start the operation selected, click the **Next** button. The application will begin copying the necessary files to your computer or deleting the selected components and data.

STEP 3. COMPLETING APPLICATION MODIFICATION, REPAIR, OR REMOVAL

The modification, repair, or removal process is displayed on the screen, after which you will be informed of its completion.

Removing the program generally requires you to restart your computer afterward, since this is necessary to account for modifications to your system. The application will ask if you want to restart your computer. Click the **Yes** button to restart immediately. To restart your computer later, click the **No** button.

REMOVING THE APPLICATION FROM THE COMMAND PROMPT

➔ To uninstall Kaspersky Anti-Virus 6.0 for Windows Servers MP4 from the command prompt, execute the following:

```
msiexec /x <package_name>
```

The installation wizard will open. You may use it to uninstall the application.

- *To uninstall the application in non-interactive mode without restarting the computer (the computer should be restarted manually after uninstalling), enter the following:*

```
msiexec /x <package_name> /qn
```

- *To uninstall the application in non-interactive mode and then restart the computer, enter the following:*

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

If you opted for password protection against uninstalling the application when you installed the application, you will need to confirm that password when uninstalling the application. Otherwise the application cannot be uninstalled.

- *To remove the application when it is password-protected, enter the following:*

```
msiexec /x <package_name> KLUNINSTPASSWD=***** – to remove the application in interactive mode;
```

```
msiexec /x <package_name> KLUNINSTPASSWD=***** /qn – to remove the application in non-interactive mode.
```


MANAGING THE APPLICATION VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit is a system for centrally managing the key administrative tasks in operating a security system for a corporate network, based on the applications included in Kaspersky Anti-Virus Open Space Security. Kaspersky Administration Kit supports all network configurations that use TCP/IP.

The application is intended for administrators of corporate computer networks and employees who are responsible for anti-virus protection in their companies.

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 is one of the Kaspersky Lab's products that can be administered through its own application interface, the command prompt (these methods are described above herein), or using Kaspersky Administration Kit (if the computer makes part of a centralized remote administration system).

To manage Kaspersky Anti-Virus via Kaspersky Administration Kit, please do the following:

- deploy *Administration Server* on the network;
- install *Administration Console* on the administrator's workstation (for more details see the Kaspersky Administration Kit Deployment Guide);
- install Kaspersky Anti-Virus and *Network Agent* (included with Kaspersky Administration Kit) on the networked computers. For more details about remote installation of the Kaspersky Anti-Virus installation package on networked computers see Kaspersky Administration Kit Deployment Guide.

Before upgrading the Kaspersky Anti-Virus administration plug-in through Kaspersky Administration Kit, close Administration Console.

Administration Console (see figure below) allows you to administer the application through Kaspersky Administration Kit. It provides a standard MMC-integrated interface, and allows the administrator to perform the following functions:

- remotely installing and uninstalling Kaspersky Anti-Virus and *Network Agent* on networked computers;
- remotely configuring Kaspersky Anti-Virus on networked computers;
- updating Kaspersky Anti-Virus databases and modules;
- managing licenses for Kaspersky Anti-Virus on networked computers;
- viewing information about the application's operation on client computers.

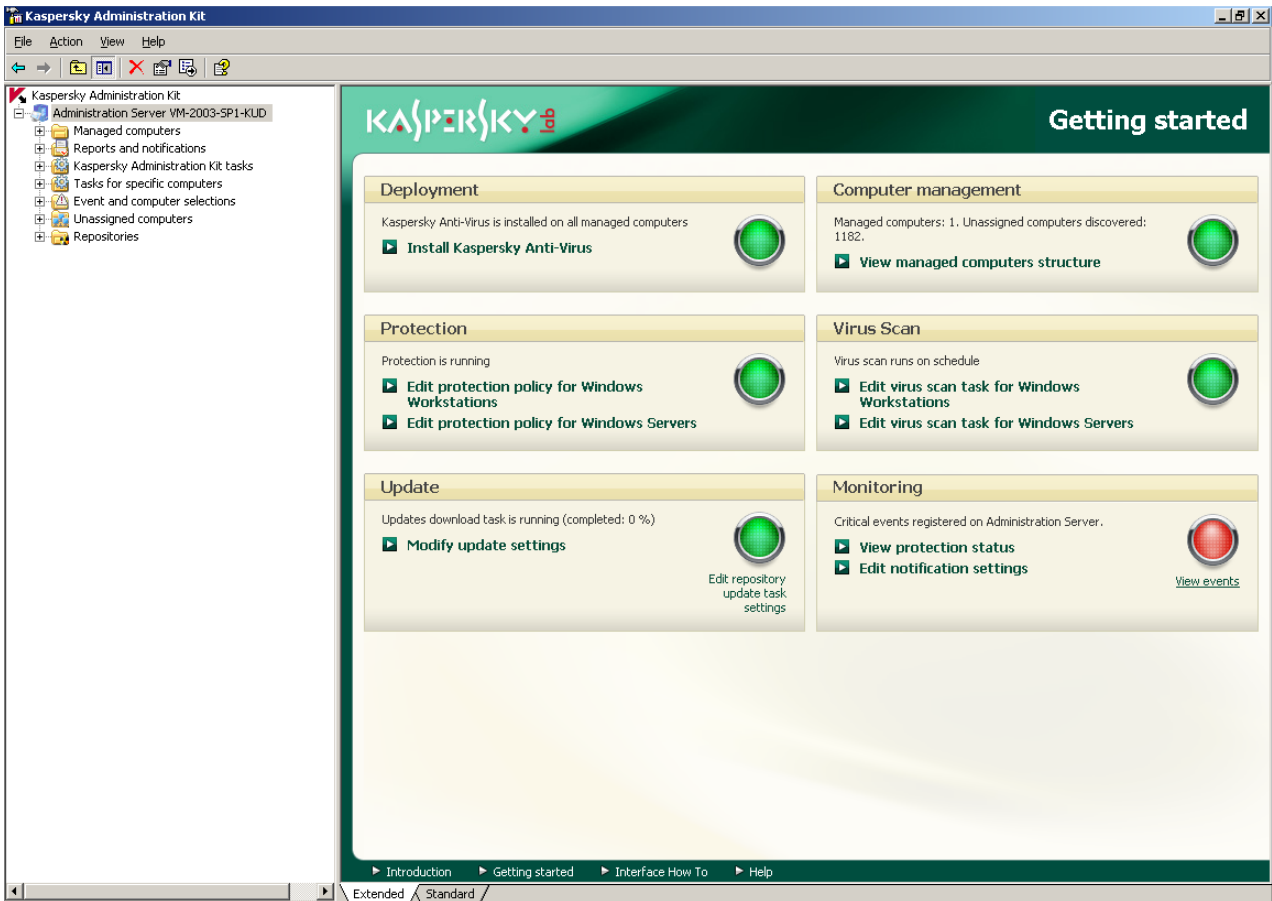


Figure 11. Kaspersky Administration Kit Administration Console

The appearance of the Kaspersky Administration Kit main window may vary depending on the operating system of the computer you are using.

When working via Kaspersky Administration Kit, the application is administered by policy settings, task settings, and application settings set by the administrator.

Named actions taken by the application are referred to as *tasks*. Based on the functions they perform, tasks are divided by *types*: virus scan tasks, application update tasks, update rollbacks, and key file installation tasks.

Each task has a collection of settings for the application that are used when it is executed. The task settings for the application that are common to all types of tasks are the *application settings*. The application settings that are specific to a task type form *task settings*. The application settings and the task settings do not overlap.

The key feature of centralized administration is grouping remote computers on the network and managing them by creating and configuring group policies.

Policy is a collection of application settings for a group, as well as a collection of restrictions on re-editing those settings when setting up the application or tasks on an individual client computer. A policy includes settings for configuring all the features of the application, with the exception of settings that are customized for specific instances of a task. Schedule settings are an example.

Thus, policies include the following settings:

- Settings common to all tasks (application settings);
- Settings common to all instances of a single task type (primarily task settings).

This means that a policy for Kaspersky Anti-Virus, the tasks for which include virus protection and scan tasks, includes all the necessary settings for configuring the application when executing both types of tasks but not, for example, a schedule for running those tasks or settings that define the scan scope.

IN THIS SECTION

Managing the application..... [115](#)

Managing tasks [119](#)

Managing policies..... [125](#)

MANAGING THE APPLICATION

Kaspersky Administration Kit gives you the opportunity to remotely start and stop Kaspersky Anti-Virus on individual client computers, as well as modifying general settings for the application, such as enabling/disabling computer protection, modifying settings for Backup and Quarantine and reporting.

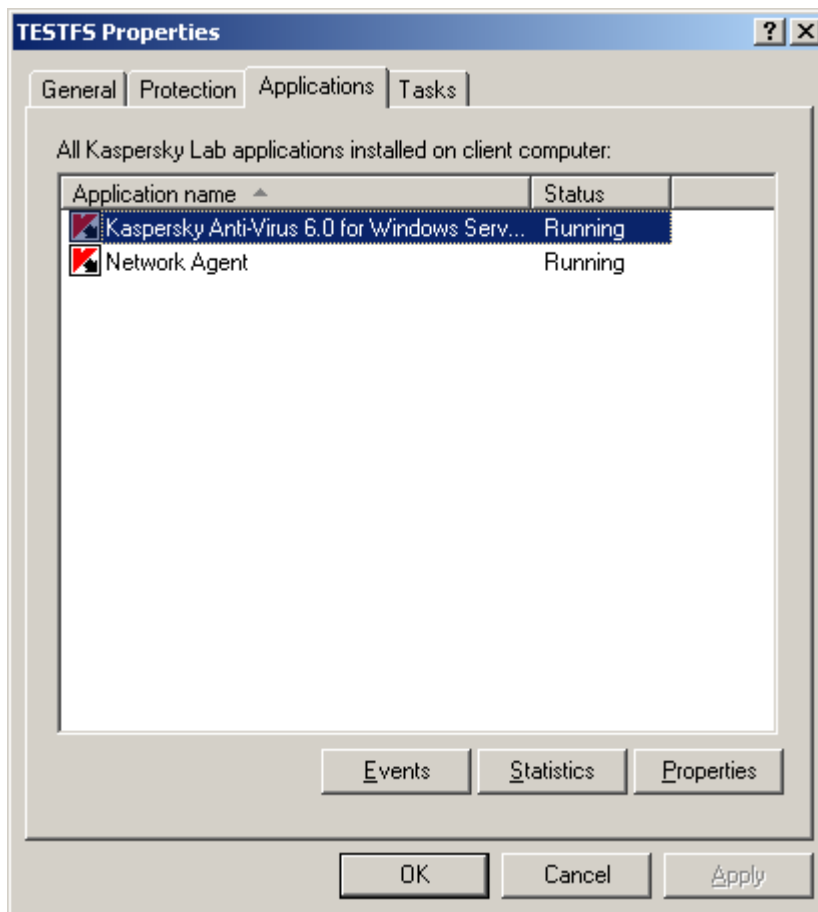


Figure 12. Client computer properties window. The **Applications** tab

➔ To manage the application, please do the following:

1. Open Kaspersky Administration Kit Administration Console.
2. Select the **Managed computers** folder with the name of the group that includes the client computer.

3. In the selected group, open the **Client computers** folder and select the computer for which you need to modify application settings.
4. Select the **Properties** command from the context menu or the corresponding item from the **Action** menu to open the client computer properties window.
5. The **Applications** tab on the properties window of the client computer displays the complete list of Kaspersky Lab applications installed on the client computer. Select **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** from the list of applications.

There are controls under the list of applications that you can use to:

- view the list of events in application operation that have occurred on the client computer and have been recorded on the Administration Server;
- view current statistics on application operation;
- modify application settings (see page [117](#)).

STARTING AND STOPPING THE APPLICATION

Kaspersky Anti-Virus 6.0 is installed and started on remote client computers from the application properties window (see figure below).

In the top part of the window, you will find the name of the application installed, information on the version, the installation date, its status (whether the application is running or stopped on the local computer), and information about the status of the threat signature database.

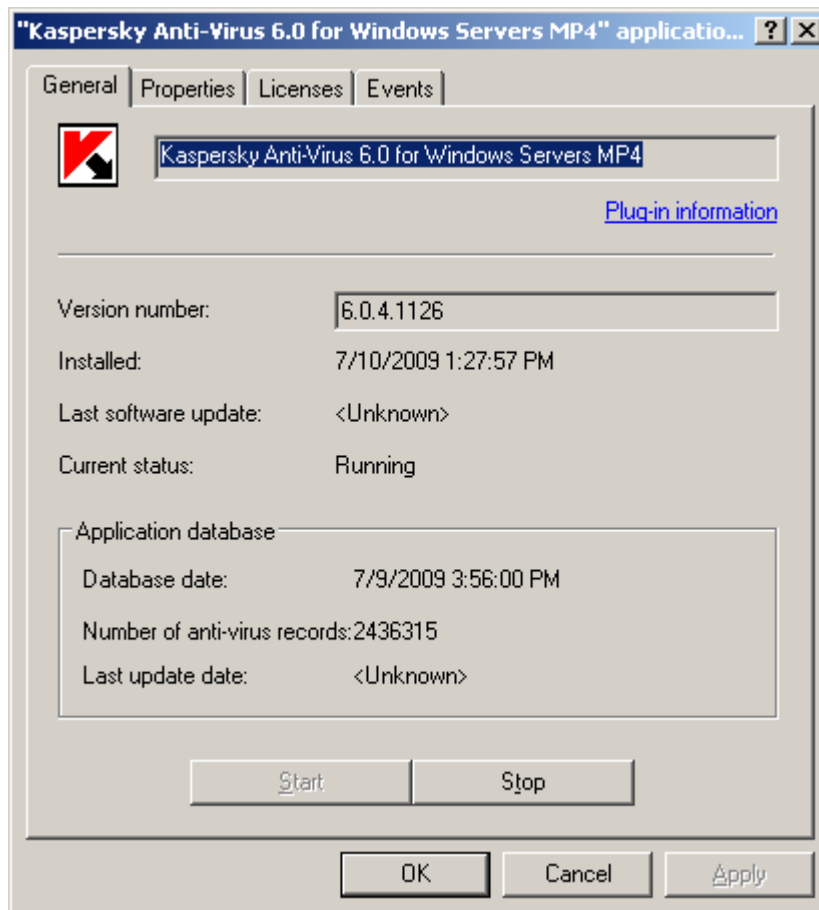


Figure 13. Application properties window. The **General** tab

➔ To stop or start the application on a remote computer, please do the following:

1. Open the properties window for the client computer (see page [115](#)) on the **Applications** tab.
2. Select **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** from the list of applications and click the **Properties** button.
3. In the application properties window that will open, on the **General** tab, click the **Stop** button to stop the application or the **Start** button to start it.

CONFIGURING APPLICATION SETTINGS

You can view and edit application settings in the application properties window on the **Properties** tab (see figure below). The other tabs are standard for the Kaspersky Administration Kit application and are covered in more details in Reference Guide.

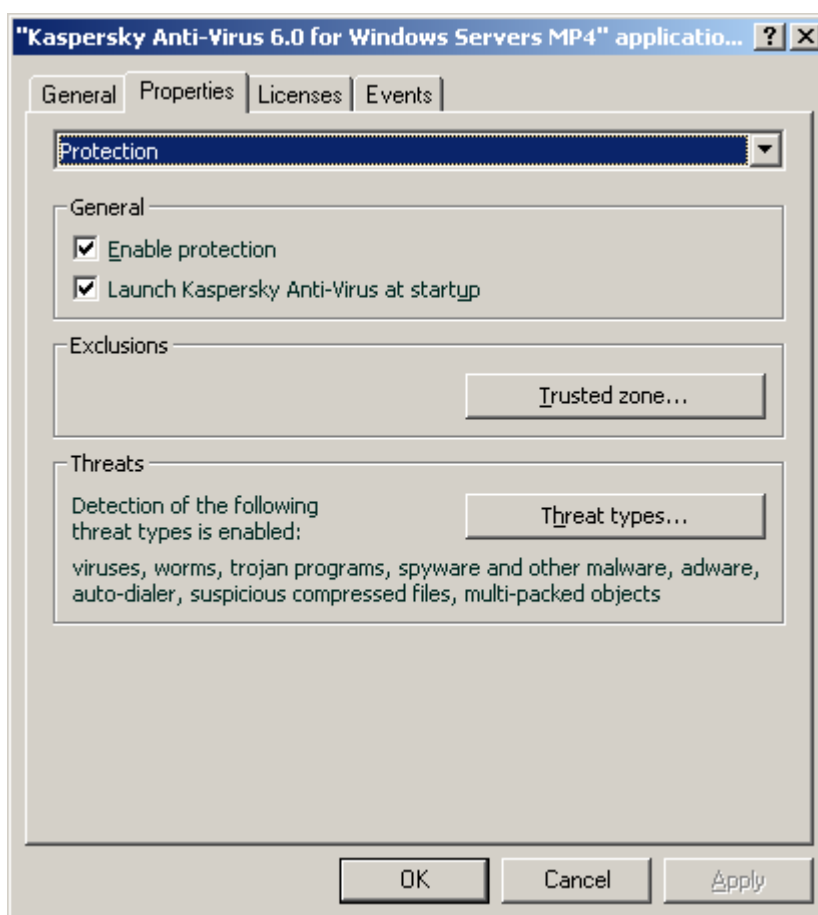


Figure 14. Application properties window. The **Properties** tab

If for the application a policy has been created (see page [126](#)) that prevents some settings from being remodified, they will be unchangeable when configuring the application.

➔ To view and edit the application settings, please do the following:

1. Open the properties window for the client computer (see page [115](#)) on the **Applications** tab.
2. Select **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** from the list of applications and click the **Properties** button.

3. In the application properties window that will open, on the **Properties** tab you can edit the general settings of Kaspersky Anti-Virus, storage and reporting settings, and network settings. To do so, select the required value from the dropdown menu in the top part of the window, and edit the settings.

SEE ALSO

Launching the application at the operating system startup.....	71
Selecting detectable threat categories.....	71
Creating a trusted zone	72
Configuring notification by email.....	82
Configuring reports.....	84
Configuring quarantine and backup.....	86

CONFIGURING SPECIFIC SETTINGS

When administering Kaspersky Anti-Virus through Kaspersky Administration Kit, you can enable/disable interactivity, configure the appearance of the application, and edit information on Technical Support. These settings can be edited in the application properties window (see figure below).

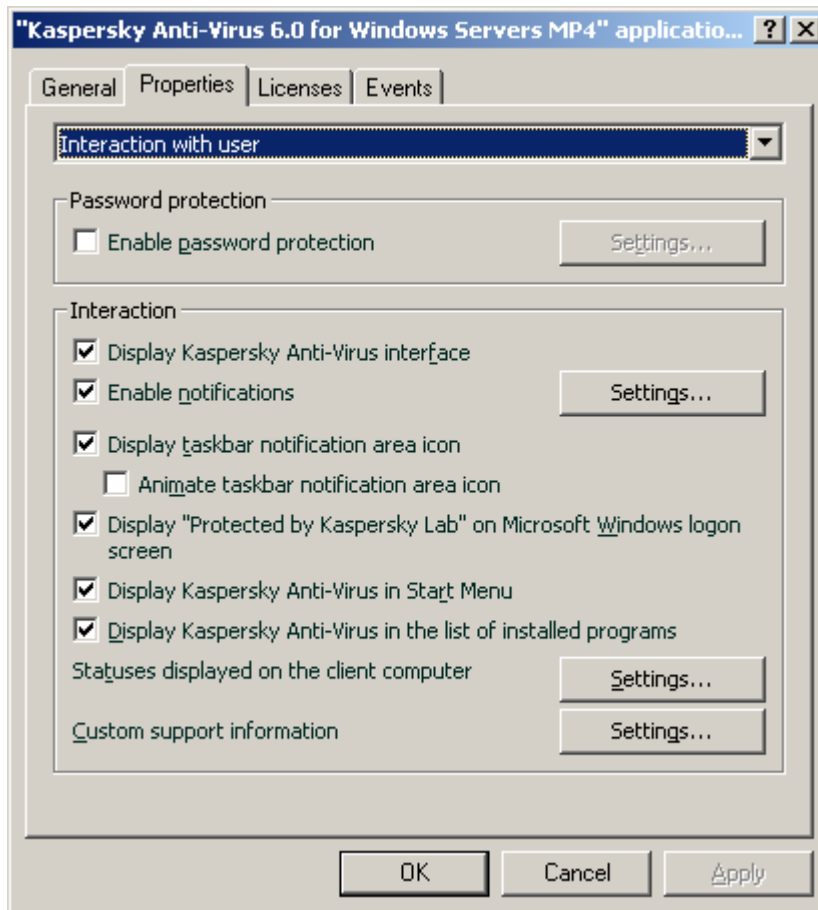


Figure 15. Application properties window. Configuring specific settings

To password-protect Kaspersky Anti-Virus, check the **Enable password protection** box in the window that will open by clicking the **Settings** button, and enter the password and area that the access restriction will cover.

To ensure protection against unauthorized removal of an application from a local computer, check the **Enable uninstall protection** box. In the window that will open by clicking the **Settings** button, enter a password for uninstall and confirm it.

To password-protect Kaspersky Anti-Virus, check the **Enable password protection** box in the window that will open by clicking the **Settings** button, and enter the password and area that the access restriction will cover.

To ensure protection against unauthorized removal of an application from a local computer, check the **Enable uninstall protection** box. In the window that will open by clicking the **Settings** button, enter a password for uninstall and confirm it.

In the **Interaction** section, you can specify the settings for user's interaction with Kaspersky Anti-Virus interface:

- If the **Disable interaction** box is unchecked, a user that works on a remote computer, will see the Kaspersky Anti-Virus icon and pop-up messages, and will have a possibility to make decisions of further actions in notification windows informing about an event. To disable the interactive mode of application operation, check the box. If there is a need to hide the fact of application's presence from the user, also check the **Hide the installed application box**.
- In the **View** window that will open by clicking the **Settings** button, you can edit the information on users technical support that is displayed in the **Support** window of Kaspersky Anti-Virus.

To change information, in the upper field enter the current text on the support provided. In the field below, you can edit the hyperlinks that are displayed in the **Useful links** section of the **Support** window that will open by clicking the **Support** link in the main window of Kaspersky Anti-Virus.

Edit the list using the **Add**, **Edit**, **Delete** buttons. Kaspersky Anti-Virus will add a new link to the top of the list. To change the order of the links in the list, use the **Move up** and **Move down** buttons.

If the window does not contain any data, the default information on technical support is not subject to editing.

In the **Application statuses** section, you can specify application statuses, which will be displayed in the main window of Kaspersky Anti-Virus. To do so, click the **Settings** button and check the boxes for required statuses in the window that will open. You can specify the monitoring periods of application databases in the same window.

In the **View** section, you can edit the settings for the interactive operation mode of Kaspersky Anti-Virus on a remote computer: showing icon over the Microsoft Windows login window, Kaspersky Anti-Virus icon animation in system tray, issuing notifications on events that occur in the application (for example, detection of a dangerous object).

If for the application a policy has been created (see page [126](#)) that prevents some settings from being remodified, they will be unchangeable when configuring the application.

➤ To view and edit the application's advanced settings, please do the following:

1. Open the client computer properties window (see page [115](#)) on the **Applications** tab.
2. Select **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** from the list of applications and click the **Properties** button.
3. In the application properties window that will open, on the **Properties** tab, select the **Interaction with user** item from the dropdown list, and edit the settings.

MANAGING TASKS

This section includes information on managing tasks for Kaspersky Anti-Virus. For more details on managing tasks via Kaspersky Administration Kit, consult the Administrator Guide for that product.

A list of system tasks is created for each networked computer when the application is being installed. This list includes protection tasks (File Anti-Virus), virus scan tasks (Full scan, Quick scan), and update tasks (updates of application databases and modules, update rollbacks).

You can manage the schedule for system tasks and edit the settings for them. These tasks cannot be deleted.

You can also create your own tasks (see page 121), such as scan tasks, application updates and update rollbacks, and key file installation tasks.

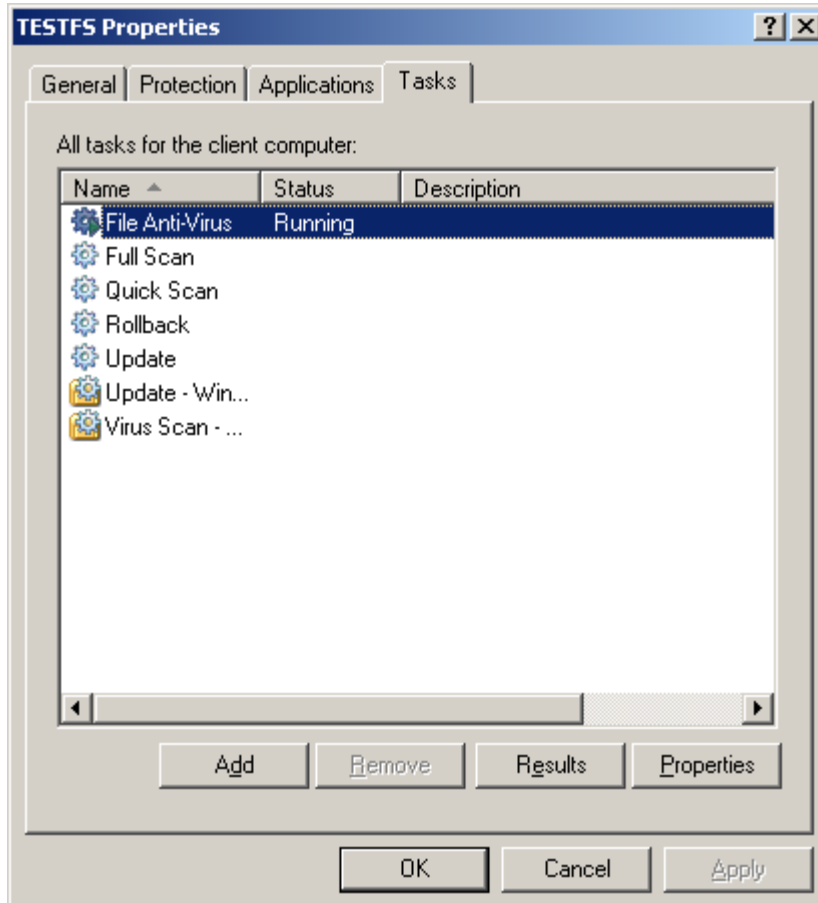


Figure 16. Client computer properties window. The **Tasks** tab

➤ To open the list of tasks created for a client computer, please do the following:

1. Open Kaspersky Administration Kit Administration Console.
2. Select the **Managed computers** folder with the name of the group that includes the client computer.
3. In the selected group, open the **Client computers** folder and select the computer for which you need to modify application settings.
4. Select the **Properties** command from the context menu or the corresponding item from the **Action** menu to open the client computer properties window.
5. In the client computer properties window that will open, select the **Tasks** tab. Here you will find the complete list of tasks created for the client computer.

STARTING AND STOPPING TASKS

Tasks are started on the client computer only if the corresponding application is running (see page [116](#)). If the application is stopped, all tasks running will be terminated.

Tasks are started and stopped automatically, according to a schedule, or manually using commands from the context menu and from the View Task Settings window. You can also pause tasks and resume them.

➔ *To start/stop/pause/resume a task manually, please do the following:*

1. Open the client computer properties window on the **Tasks** tab.
2. Select the required task and open the context menu for it. Select the **Start** item to start the task or the **Stop** item to stop it. You can also use the corresponding items in the **Action** menu.

You cannot pause or resume a task from the context menu.

or

Select the required task from the list and click the **Properties** button. You can use the buttons on the **General** tab in the task properties window that will open to start, stop, pause, or resume a task.

CREATING TASKS

When working with the application via Kaspersky Administration Kit, you can create the following types of tasks:

- local tasks defined for individual client computers;
- group tasks defined for client computers that belong to administration groups;
- tasks for sets of computers that are defined for computers outside of administration groups;
- Kaspersky Administration Kit tasks are specific tasks for the Update Server: update download tasks, backup tasks, and report sending tasks.

Computer group tasks are only performed on the selected set of computers. If new client computers are added to a group with computers for which a remote installation task has been created, this task will not run for them. You should create a new task or make appropriate changes to the settings of the existing task.

You can take the following actions on tasks:

- specifying tasks settings;
- monitoring task execution;
- copying and moving tasks from one group to another, and also deleting them using the standard commands **Copy/Paste**, **Cut/Paste**, **Delete** from the context menu, or the same commands from the **Action** menu;
- importing and exporting tasks.

Consult the Kaspersky Administration Kit Reference Guide for more information on working with tasks.

➔ *To create a local task, please do the following:*

1. Open the properties window of the required client computer on the **Tasks** tab.

2. Click the **Add** button.
3. The New Task Wizard will then start (see page [122](#)). Please follow its instructions.

➤ *To create a group task, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.
3. In the group you have selected, open the **Group tasks** folder, where you will find all of the tasks created for that group.
4. Open the New Task Wizard by clicking the **Create a new task** link in the taskbar. The specifics of creating group tasks are covered in the Kaspersky Administration Kit Reference Guide.

➤ *To create a task for a group of computers (a Kaspersky Administration Kit task), please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. Select the **Tasks for specific computers** folder (**Kaspersky Administration Kit tasks**).
3. Open the New Task Wizard by clicking the **Create a new task** link in the taskbar. The specifics of creating Kaspersky Administration Kit tasks and tasks for groups of computers are covered in the Kaspersky Administration Kit Reference Guide.

LOCAL TASK WIZARD

The Local Task Wizard starts when you select the corresponding commands from the context menu for the client computer or from the properties window for that computer.

This wizard consists of a series of boxes (steps) navigated using the **Back** and **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To cancel the wizard at any stage, use the **Cancel** button.

STEP 1. ENTERING GENERAL DATA ON THE TASK

The first wizard window is introductory: all you enter here is the name of the task (the **Name** field).

STEP 2. SELECTING AN APPLICATION AND TASK TYPE

At this step, you should specify the application for which the task is being created (Kaspersky Anti-Virus 6.0 for Windows Servers MP4, or Administration Agent). You should also select the task type. The possible tasks for Kaspersky Anti-Virus 6.0 are:

- *Scan for viruses* – task of virus scan of the areas specified by the user.
- *Update* – retrieves and applies update packages for the application.
- *Update Rollback* – rolls back to the latest application update.
- *Key file installation* - installation of a key file for a new license as needed to operate the application.

STEP 3. CONFIGURING THE SELECTED TASK TYPE

Depending on the task type selected at the previous step, the contents of the settings window may vary.

The [virus scan tasks](#) require you to specify the action that Kaspersky Anti-Virus will take if it detects a malicious object (see page [49](#)) and requires you to create a list of objects to be scanned (see page [48](#)).

For database and application module update tasks, you should specify the source that will be used to download updates (see page [60](#)). The default update source is the Kaspersky Administration Kit update server.

Update rollback tasks have no specific settings.

For license key installation tasks, specify the path to the key file with the **Browse** button. In order to add a file as a license key for an additional license, check the corresponding box. The additional license key will take effect when the active license key expires.

Information about the specified license (license number, type, and expiration date) is displayed in the field below.

STEP 4. CONFIGURING A SCHEDULE

After configuring the tasks, you will be offered to configure the automatic task run schedule.

To do so, select the frequency for running the task from the dropdown menu in the schedule settings window and modify the schedule settings in the bottom part of the window.

STEP 5. COMPLETING THE TASK CREATION

The last window of the wizard will inform you that you have successfully created the task.

CONFIGURING TASKS

Configuring application tasks via the Kaspersky Administration Kit interface is similar to configuring via the local Kaspersky Anti-Virus interface, except for the settings that are edited individually for each user, such as scan tasks run schedule, or settings specific to Kaspersky Administration Kit, such as settings that allow/block managing local scan tasks by the users.

If for the application a policy has been created (see page [126](#)) that prevents some settings from being remodified, they will be unchangeable when configuring the application.

All the tabs in the task properties window besides the **Properties** tab (see figure below) are standard for Kaspersky Administration Kit and are covered in more details in the Reference Guide. The **Properties** tab contains specific settings for Kaspersky Anti-Virus. The contents of this tab vary depending on the task type selected.

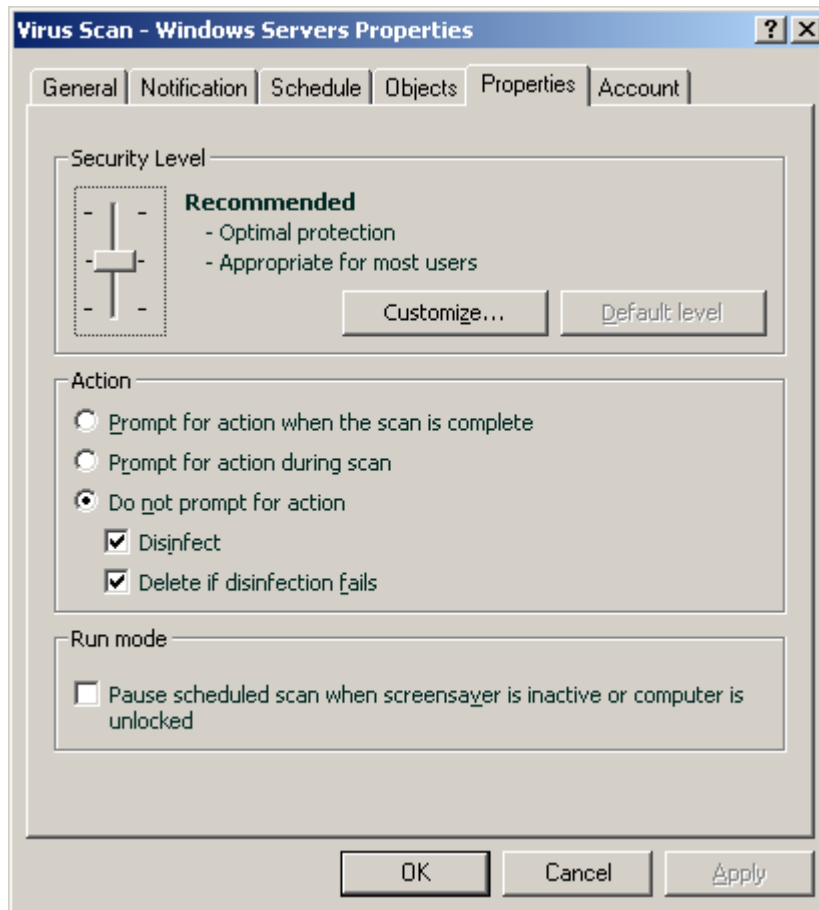


Figure 17. Task properties window. The **Properties** tab

➤ To view and edit local tasks, please do the following:

1. Open the client computer properties window on the **Tasks** tab.
2. Select a task from the list and click the **Properties** button. As a result, the task settings window will open.

➤ To view the group tasks, please do the following:

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.
3. In the group you have selected, open the **Group tasks** folder, where you will find all of the tasks created for that group.
4. Select the required task from the console tree to view and edit its properties.

The taskbar will display comprehensive information on the task and the links for managing task execution and editing its settings. The specifics of creating group tasks are described in the Kaspersky Administration Kit Reference Guide.

➤ To view tasks for a group of computers (a Kaspersky Administration Kit task), please do the following:

1. Open Kaspersky Administration Kit Administration Console.



2. Select the **Tasks for specific computers** folder (**Kaspersky Administration Kit tasks**).
3. Select the required task from the console tree to view and edit its properties.

The taskbar will display comprehensive information on the task and the links for managing task execution and editing its settings. The specifics of Kaspersky Administration Kit tasks and tasks for sets of computers can be found in the Kaspersky Administration Kit Reference Guide.

MANAGING POLICIES

Setting up policies allows you to apply universal application and task settings to client computers that belong to a single administration group.

This section includes information on creating and configuring policies for Kaspersky Anti-Virus 6.0 for Windows Servers MP4. For more details on the concept of managing policies through Kaspersky Administration Kit, see the Administrator Guide for the application.

When creating and configuring a policy, you can fully or partially block settings from being edited in policies for nested groups, task settings, and application settings. To do so, click the  button. It should change to  for settings that are locked.

➔ *To open the list of policies for Kaspersky Anti-Virus, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. Select the **Managed computers** folder with the name of the group that includes the client computer.
3. In the group you have selected, open the **Policies** folder, where you will find all of the policies created for that group.

CREATING POLICIES

When working with Kaspersky Anti-Virus via Kaspersky Administration Kit, you may create the following types of policies:

You can take the following actions on policies:

- configuring policies;
- copying and moving policies from one group to another, and also deleting them using the standard commands **Copy/Paste**, **Cut/Paste**, **Delete** from the context menu, or the same commands from the **Action** menu;
- importing and exporting policy settings.

Working with policies is covered in more details in the Kaspersky Administration Kit Reference Guide.

➔ *To create a policy, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.
3. In the group you have selected, open the **Policies** folder, where you will find all of the policies created for that group.
4. Open the New Task Wizard by clicking the **Create a new policy** link in the taskbar.
5. The New Task Wizard will then start in the window that will open (see page [126](#)): and follow its instructions.

POLICY CREATION WIZARD

The Policy Wizard can be started by selecting the corresponding action from the context menu of the **Policies** folder of the required administration group, or by clicking the link in the results panel (for the **Policies** folders).

This wizard consists of a series of boxes (steps) navigated using the **Back** and **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To cancel the wizard at any stage, use the **Cancel** button.

STEP 1. ENTERING GENERAL DATA ON THE POLICY

The first wizard windows are welcome windows. Here you should specify the name of the policy (the **Name** field) and select **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** from the **Application name** dropdown menu.

If you run the Policy Creation Wizard from the **Policies** node of the taskbar (using the **Create a new Kaspersky Anti-Virus for Windows Servers MP4 policy**), you will not be able to select an application.

If you want to create a policy based on the settings of an existing policy created for the previous version of the application, check the **Take settings from existing policy** box and select the policy whose settings should be used in the new policy. To select a policy, click the **Select** button, which will open the list of existing policies that you may use when creating a new one.

STEP 2. SELECTING THE POLICY STATUS

In this window, you will be offered to specify the status of the policy after it is created, selecting one of the following options: active policy or inactive policy. Consult the Kaspersky Administration Kit Reference Guide for more details on policy statuses.

Several policies may be created for a single application in a group, but only one of them can be the current (active) policy.

STEP 3. IMPORTING THE APPLICATION SETTINGS

If you have a file with application settings saved earlier, you can specify the path to it using the **Load** button; the wizard windows displayed hereafter will show the imported settings.

STEP 4. CONFIGURING THE PROTECTION

At this step, you can enable/disable or configure protection components that will be used in the policy.

All protection components are enabled by default. To disable any of the components, uncheck the box next to it. To fine-tune a protection component, select it from the list and click the **Configure** button.

STEP 5. CONFIGURING PASSWORD PROTECTION

In this wizard window, you will be offered to configure password protection applied to operations with the application and to uninstallation.

STEP 6. CONFIGURING THE TRUSTED ZONE

In this window of the wizard, you will be offered to configure the trusted zone: add the software used for network administration to the list of trusted applications, and exclude several file types from scan.

STEP 7. CONFIGURING THE INTERACTION WITH THE USER





At this step, you can specify the settings for interaction between the user and Kaspersky Anti-Virus:

- displaying the application's interface on a remote computer;
- notifying the user about events;
- displaying the application icon in the taskbar notification area and animating it;
- displaying "Protected by Kaspersky Lab" on Microsoft Windows logon screen;
- displaying the application in the Start menu;
- displaying the application in the list of applications installed.

STEP 8. COMPLETING THE POLICY CREATION

The final window of the wizard will inform you that you have successfully created the policy.

Once the wizard closes, the policy for the application will be added to the **Policies** folder of the corresponding group, becoming visible in the console tree.

You can edit the settings of the policy created and set restrictions on modifying its settings using the  and  buttons for each group of settings. If the  icon is displayed, the client computer user will not be able to edit the settings. If the  icon is displayed, the user will be able to edit the settings. The policy will be applied to client computers the first time the clients synchronize with the server.

CONFIGURING THE POLICY

At the editing stage, you can modify the policy and block modification of the settings in nested group policies, and in the application and task settings. Policy settings can be edited in the policy properties window (see figure below).

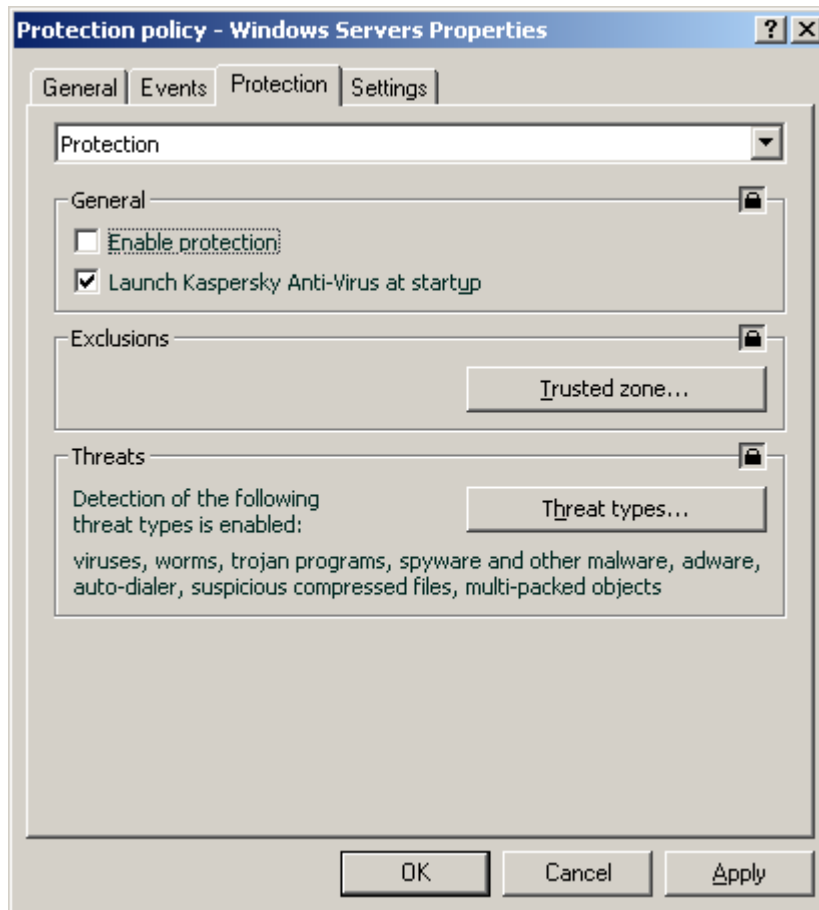


Figure 18. Policy properties window. The **Protection** tab

All the tabs, except for the **Protection** and **Settings** tabs, are standard for Kaspersky Administration Kit. They are covered in more details in the Administrator Guide.

Policy settings for Kaspersky Anti-Virus 6.0 include application settings (see page 117) and task settings. The **Settings** tab displays the application settings and the **Protection** tab displays the task settings.

To edit settings, select the required value from the dropdown menu in the top part of the window and set it.

➔ To view and edit policies settings, please do the following:

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.
3. In the group you have selected, open the **Policies** folder, where you will find all of the policies created for that group.
4. Select the required policy from the console tree to view and edit its properties.
5. The taskbar will display comprehensive information on the policy and the links for managing the policy status and editing its settings.

or

Open the context menu for the policy selected and use the **Properties** item to open the policy settings window of Kaspersky Anti-Virus.

The specifics of working with policies can be found in the Kaspersky Administration Kit Reference Guide.

USING THIRD-PARTY CODE

When creating Kaspersky Anti-Virus, third-party code has been used.

IN THIS SECTION

Boost-1.30.0 library	131
LZMA SDK 4.40, 4.43 library	131
Windows Template Library 7.5	131
Windows Installer XML (WiX) toolset 2.0 library	132
ZIP-2.31 library	135
ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 library	136
UNZIP-5.51 library	136
LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 library	137
LIBJPEG-6B library	139
LIBUNGIF-4.1.4 library	141
MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 library	141
MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 library	141
INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 library	141
CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 library	142
COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum library	142
PLATFORM INDEPENDENT IMAGE CLASS library	142
FLEX PARSER (FLEXLEXER)-V. 1993 library	143
ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 library	143
STDSTRING- V. 1999 library	144
T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 library	144
NTSERVICE- V. 1997 library	145
SHA-1-1.2 library	145
COCOA SAMPLE CODE- V. 18.07.2007 library	146
PUTTY SOURCES-25.09.2008 library	146
Other information	147

BOOST-1.30.0 LIBRARY

When creating the application, the Boost-1.30.0 library has been used.

Copyright (C) 2003, Christof Meerwald

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LZMA SDK 4.40, 4.43 LIBRARY

When creating the application, the LZMA SDK 4.40, 4.43 library has been used.

WINDOWS TEMPLATE LIBRARY 7.5

When creating the application, the Windows Template Library 7.5 has been used.

Copyright (C) 2006, Microsoft Corporation

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce", "reproduction", "derivative works", and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

WINDOWS INSTALLER XML (WIX) TOOLSET 2.0 LIBRARY

When creating the application, the Windows Installer XML (WiX) toolset 2.0 library has been used.

Copyright (C) 2009, Microsoft Corporation

 Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the

Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZIP-2.31 LIBRARY

When creating the application, the ZIP-2.31 library has been used.

Copyright (C) 1990-2005, Info-ZIP

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

<ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 LIBRARY

When creating the application, the ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 library has been used.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

UNZIP-5.51 LIBRARY

When creating the application, the UNZIP-5.51 library has been used. Copyright (c) 1990-2004 Info-ZIP.

Copyright (c) 1990-2004, Info-ZIP

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herboth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered

versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

LIBRARY

When creating the application, the LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 library has been used.

 This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg" (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

LIBJPEG-6B LIBRARY

When creating the application, the LIBJPEG-6B library has been used.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

- (1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

- (2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

- (3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us. Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBUNGIF-4.1.4 LIBRARY

When creating the application, the LIBUNGIF-4.1.4 library has been used.

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 LIBRARY

When creating the application, the MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 library has been used.

MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 LIBRARY

When creating the application, the MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 library has been used.

INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 LIBRARY

When creating the application, the INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 library has been used.

Copyright (C) 1991-2, RSA Data Security, Inc.

RSA's MD5 disclaimer

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 LIBRARY

When creating the application, the CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 library has been used.

Copyright 2001-2004 Unicode, Inc.

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM LIBRARY

When creating the application, the COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum library has been used.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware,Shareware,Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

PLATFORM INDEPENDENT IMAGE CLASS LIBRARY

When creating the application, the PLATFORM INDEPENDENT IMAGE CLASS library has been used.

Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx)

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any

necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

FLEX PARSER (FLEXLEXER)-V. 1993 LIBRARY

When creating the application, the FLEX PARSER (FLEXLEXER)-V. 1993 library has been used.

Copyright (c) 1993 The Regents of the University of California

This code is derived from software contributed to Berkeley by

Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 LIBRARY

When creating the application, the ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 library has been used.

Copyright (C) 2009, Microsoft Corporation

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License <http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL>.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

STDSTRING- V. 1999 LIBRARY

When creating the application, the STDSTRING- V. 1999 library has been used.

Copyright (C) 1999, Joseph M. O'Leary

 This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your \$30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 LIBRARY

When creating the application, the T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 library has been used.

Copyright (C) 2003-2006, Alberto Demichelis

 This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

NTSERVICE- V. 1997 LIBRARY

When creating the application, the NTSERVICE- V. 1997 library has been used.

Copyright (C) 1997, Joerg Koenig and the ADG mbH, Mannheim, Germany

 Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "///
 TCW MOD"

SHA-1-1.2 LIBRARY

When creating the application, the SHA-1-1.2 library has been used.

Copyright (C) 2001, The Internet Society

 This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE

ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

COCOA SAMPLE CODE- V. 18.07.2007 LIBRARY

When creating the application, the Cocoa sample code- v. 18.07.2007 library has been used.

Copyright (C) 2007, Apple Inc

Disclaimer: IMPORTANT: This Apple software is supplied to you by Apple Inc. ("Apple")

in consideration of your agreement to the following terms, and your use, installation, modification or redistribution of this Apple software constitutes acceptance of these terms. If you do not agree with these terms, please do not use, install, modify or redistribute this Apple software.

In consideration of your agreement to abide by the following terms, and subject to these terms, Apple grants you a personal, non – exclusive license, under Apple's copyrights in this original Apple software (the "Apple Software"), to use, reproduce, modify and redistribute the Apple Software, with or without modifications, in source and / or binary forms; provided that if you redistribute the Apple Software in its entirety and without modifications, you must retain this notice and the following text and disclaimers in all such redistributions of the Apple Software. Neither the name, trademarks, service marks or logos of Apple Inc. may be used to endorse or promote products derived from the Apple Software without specific prior written permission from Apple. Except as expressly stated in this notice, no other rights or licenses, express or implied, are granted by Apple herein, including but not limited to any patent rights that may be infringed by your derivative works or by other works in which the Apple Software may be incorporated.

The Apple Software is provided by Apple on an "AS IS" basis.

APPLE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON - INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH YOUR PRODUCTS.

IN NO EVENT SHALL APPLE BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) ARISING IN ANY WAY OUT OF THE USE, REPRODUCTION, MODIFICATION AND / OR DISTRIBUTION OF THE APPLE SOFTWARE, HOWEVER CAUSED AND WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PUTTY SOURCES-25.09.2008 LIBRARY

When creating the application, the PUTTY SOURCES-25.09.2008 library has been used. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified <http://www.opensource.org/licenses/> and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

OTHER INFORMATION

Crypto C program library, developed by CryptoEx OOO (<http://www.cryptox.ru>), is used to check digital signature.

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 source@kaspersky.com.

GLOSSARY

A

ACTIVE LICENSE

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with the active status.

ADDITIONAL LICENSE

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

ARCHIVE

File "containing" one or several other objects which can also be archives.

AVAILABLE UPDATES

A set of updates for Kaspersky Lab application modules including critical updates accumulated over a period of time and changes to the application's architecture.

B

BACKUP

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

BACKUP COPY

Creating a backup copy of a file before any processing and putting the copy into the backup storage area with the possibility of restoring the file later, for example, to scan it with updated databases.

BACKUP STORAGE

A special storage folder for copies of Administration Server data created using a backup utility.

BLACK LIST OF KEY FILES

A database containing information on blacklisted Kaspersky Lab key files whose owners violated the terms of the license agreement and information on key files that were issued but for some reason were not sold or were replaced. A blacklist file is necessary for the operation of Kaspersky Lab applications. File contents is updated together with the databases.

BLOCKING THE OBJECT

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

BOOT-VIRUS

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

C

COMPRESSED FILE

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

D**DANGEROUS OBJECT**

Object containing a virus. You are advised not to access these objects, because it may result in an infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

DATA FOLDER

The folder containing service folders and databases needed for working with the application. If the data folder is moved, all of the information that it includes must be saved at the new location.

DATABASE UPDATES

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

DATABASES

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

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 disinfecting.

DISINFECTING OBJECTS ON RESTART

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original infected object with the disinfected copy after the next system restart.

DISK BOOT SECTOR

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disc's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows to scan boot sectors for viruses and disinfect them if an infection is found.

E**EVENT SEVERITY LEVEL**

Description of the event, logged during the operation of Kaspersky Lab application. There exist four severity levels:

- **Critical event.**
- **Functional failure.**
- **Warning.**
- **Informational message.**

Events of the same type may have different severity levels, depending on the situation when the event occurred.

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.

F**FALSE ALARM**

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

FILE MASK

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

H**HEADER**

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and the recipient, and the date.

HEURISTIC ANALYZER

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

The use of heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

I**iCHECKER TECHNOLOGY**

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remain unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive scanned by Kaspersky Lab application which has been assigned the *not infected* status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive will be re-scanned.

Limitations of iChecker technology:

this technology does not work with large-size files since it is faster to scan a file than check whether it was modified since it had been last scanned;

the technology supports a limited number of formats (.exe, .dll, .lnk, .tff, .inf, .sys, .com, .chm, .zip, .rar).

INCOMPATIBLE APPLICATION

An antivirus application from a third party developer or a Kaspersky Lab application that does not support management through Kaspersky Administration Kit.

INFECTED OBJECT

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

INTERCEPTOR

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

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.

KEY FILE

File with the .key extension, which is your personal "key", necessary for working with Kaspersky Lab application. A key file is included with the product if you have purchased it from Kaspersky Lab distributors, or it is emailed to you if you have purchased the product at eStore.

L**LICENSE VALIDITY PERIOD**

Period of time during which you are able to use all of the features of your Kaspersky Lab's application. License validity period generally accounts for one calendar year from the date of its installation. After the license expires, the application will have reduced functionality. You will not be able to update the application databases.

M**MAXIMUM PROTECTION**

Security level for your computer corresponding to the most complete protection that an application can provide. At this protection level, all files on the computer, removable storage media, and network drives are scanned for viruses if connected to the computer.

MESSAGE DELETION

Method of processing an email message that contains spam signs, at which the message is physically removed. This method is advised to apply to messages unambiguously containing spam. Before deleting a message, a copy of it is saved in the backup (unless this option is disabled).

MONITORED OBJECT

A file transferred via HTTP, FTP, or SMTP protocols across the firewall and sent to a Kaspersky Lab application to be scanned.

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. Quarantined objects can be scanned using updated Anti-Virus databases, analyzed by the administrator, or sent to Kaspersky Lab.

O**OBJECT DISINFECTION**

The method used for processing infected objects that results in complete or partial data recovery, or the decision that the objects cannot be disinfected. Disinfection of objects is performed 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.

OLE OBJECT

An attached object or an object embedded into another file. Kaspersky Lab application allows to scan OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table will be scanned as an OLE object.

ON-DEMAND SCAN

Operating mode of the Kaspersky Lab application that is initiated by the user and can target any files on the computer.

P**POTENTIALLY INFECTABLE OBJECT**

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the .com, .exe, .dll extensions, etc. The risk of activating any malicious code in such files is fairly high.

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.

Q**QUARANTINE**

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

R**REAL-TIME PROTECTION**

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

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.

S**SIMPLE OBJECT**

Email body or simple attachments, for example, an executable file. Also see container objects.

SKIPPING OBJECTS

A method of processing in which an object is passed on to the user without any changes. If event logging is enabled for this event type, information about the object detected will be logged in the report.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which could lead to, for example, blocking your access to the operating system.

STORAGE SCAN

Scanning the email stored on the mail server and the contents of shared folders using the latest version of the database. The scan runs in the background and can be run using a schedule or on demand. All shared folders and mailbox storage are scanned. New viruses may be detected during the scan about which no information was in the database at the time of previous scans.

SUBNET MASK

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

SUSPICIOUS OBJECT

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

T**TRUSTED PROCESS**

Application process whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects launched, opened, or saved by the trusted process will be scanned.

U**UNKNOWN VIRUS**

A new virus about which there is no information in the databases. Generally unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

UPDATE

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

UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

URGENT UPDATES

Critical updates to Kaspersky Lab application modules.

V**VIRUS ACTIVITY THRESHOLD**

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, will be considered excessive virus activity and a threat of a virus outbreak. This feature is significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

KASPERSKY LAB

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

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

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

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

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

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

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

Kaspersky Lab official site: <http://www.kaspersky.com>

Virus Encyclopedia: <http://www.viruslist.com>

Anti-Virus Lab: newvirus@kaspersky.com
(only for sending archives of suspicious objects)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>
(for queries to virus analysts)

LICENSE AGREEMENT

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

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

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

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

- 1.1. **Software** means software including any Updates and related materials.
- 1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.
- 1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.
- 1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, "*You*" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "*organization*," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.
- 1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.
- 1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.
- 1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.
- 1.8. **Software Acquisition** means purchase of the Software or acquisition of the Software on terms defined in additional agreement including acquisition at no charge.

2. Grant of License

- 2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:
Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the

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

- 2.2. If the Software was acquired on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package or as specified in additional agreement.
- 2.3. If the Software was acquired via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You acquired the License to the Software or as specified in additional agreement.
- 2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.
- 2.5. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was acquired on a physical medium) or specified during acquisition (if the Software was acquired via the Internet):
 - Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
 - Technical Support via the Internet and Technical Support telephone hotline.

3. **Activation and Term**

- 3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.
- 3.2. If the Software was acquired on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement or as specified in additional agreement.
- 3.3. If the Software was acquired via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during acquisition or as specified in additional agreement.
- 3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline.
- 3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.
- 3.6. If You have acquired the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.
- 3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.
- 3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.
- 3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. **Technical Support**

The Technical Support described in Clause 2.5 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).

Technical support service: <http://support.kaspersky.com>

5. **Limitations**

- 5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its

suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

- 5.2. You shall not transfer the rights to use the Software to any third party except as set forth in additional agreement.
- 5.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in additional agreement.
- 5.4. You shall not rent, lease or lend the Software to any third party.
- 5.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.
- 5.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.
- 5.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

6. Limited Warranty and Disclaimer

- 6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.
- 6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.
- 6.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.
- 6.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.5 of this Agreement.
- 6.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.
- 6.6. THE SOFTWARE IS PROVIDED "AS IS" AND THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE Rightholder AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE Rightholder MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE Rightholder .

7. Exclusion and Limitation of Liability

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

(INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

8. GNU and Other Third Party Licenses

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

9. Intellectual Property Ownership

- 9.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.
- 9.2 You acknowledge that the source code, activation code and/or license key file for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.
- 9.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

10. Governing Law; Arbitration

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or

application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

11. Period for Bringing Actions

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

12. Entire Agreement; Severability; No Waiver

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

13. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

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

INDEX

A

Actions to be performed on the objects	38
Application Interface	31
Application self-defense	78

B

Backup	86
--------------	----

C

Context menu	32
--------------------	----

D

Detectable threat categories	71
------------------------------------	----

F

File Anti-Virus	
heuristic analysis	40
operation algorithm	37
pausing	43
protection scope	39
reaction to the threat	38
scan mode	42
scan of compound files	41
scan optimization	41
scan technology	42
security level	38
statistics on component operation	44

H

Heuristic analysis	
File Anti-Virus	40

I

iSwift files	80
--------------------	----

K

Kaspersky Lab	10
---------------------	----

M

Main application window	33
-------------------------------	----

N

Notifications	81
---------------------	----

O

Operation algorithm	
File Anti-Virus	37

P

Protection scope	
File Anti-Virus	39

Q

Quarantine.....	85, 86
Quarantine and Backup.....	85, 86

R

Reaction to the threat	
File Anti-Virus	38
virus scan.....	49
Reports.....	84
Rescue Disk	87, 88, 89
Restoring the default settings	43
Restricting access to the application	79

S

Scan	
action to be performed on detected object.....	49
automatic launch of skipped task.....	53, 55
on schedule	55
pause task	53, 54
run mode.....	54, 55
scan of compound files	52
scan optimization	51
scan technologies	52
security level.....	49
type of objects to scan	50
Security level	
File Anti-Virus	38
Statistics on component operation	
File Anti-Virus	44

T

Task start	
scan	47, 54, 55
update.....	59, 61, 62, 63
Taskbar notification area icon.....	31
Trusted zone	
exclusion rules.....	72
trusted applications	72, 74

U

Update	
from a local folder	63
manually	59
on schedule	63
regional settings.....	61
rolling back the last update	60
run mode.....	61, 62, 63
update object	62
update source	60
using proxy server	61