KASPERSKY LAB

Kaspersky Anti-Virus® Personal Pro 5.0

USER'S GUIDE

KASPERSKY ANTI-VIRUS® PERSONAL PRO 5.0

User's Guide

http://www.kaspersky.com

Revision date: April, 2006

Contents

CHAPTER 1. INTRODUCTION

1.1. Computer viruses and malicious computer programs

As modern computer technology and communications tools develop, hackers have more opportunities for spreading threats. Let’s take a closer look at them:

The Internet

The Internet is unique, since it is no one’s property and has no geographical borders. In many ways, this has promoted development of countless web resources and the exchange of information. Today, anyone can access data on the Internet or create their own webpage.

However, these very features of the worldwide web give hackers the ability to commit crimes on the Internet, making them difficult to detect and punish as they go.

Hackers place viruses and other malicious programs on Internet sites and disguise it as useful freeware. Furthermore, scripts that run automatically when you open a webpage can execute dangerous actions on your computer, including modifying the system registry, stealing personal data, and installing malicious software.

By using network technologies, hackers can attack remote PCs and company servers. These attacks can cause parts of your system to malfunction or could provide hackers with complete access to your system and thereby to the information stored on it. They can also use it as part of a zombie network.

Ever since it became possible to use credit cards and e-money through the Internet in online stores, auctions, and bank homepages, online scams have surfaced as one of the most common crimes.

Intranet

Your intranet is your internal network, specially designed for handling information within a company or a home network. An intranet is a unified space for storing, exchanging, and accessing information for all the computers on the network. This means that if one computer on the network is infected, the others are at great risk of infection. To avoid such situations, both the network perimeter and each individual computer must be protected.

E-mail

Since practically every computer has mail clients installed on it and since malicious programs exploit the contents of electronic address books, conditions are usually right for spreading malicious programs. The user of an infected computer, himself oblivious to the fact, might send infected e-mails to friends or coworkers who in turn send more infected e-mails. It is common that infected file documents go undetected at are sent out with business information from a large company. When this occurs, more than a handful of people are infected. It could be hundreds or thousands, all of whom then send the infected files to tens of thousands of subscribers.

Beyond the threat of malicious programs lies the program of electronic junk mail, or spam. Although not a direct threat to your computer, spam increases the load on mail servers, eats up bandwidth, fills up your mailbox, and wastes working hours, thereby incurring financial harm.

Also, note that hackers have begun using mass mailing programs and social engineering methods to convince users to open e-mails or click a link to a certain website. It follows that spam filtration capabilities are both for stopping junk mail and for counteracting new types of online scans, such as phishing, and for stopping the spread of malicious programs.

Removable storage media

Removable media (floppies, CD-ROMs, and USB flash drives) are widely used for storing and transmitting information.

When you open a file that contains malicious code from a removable storage device, you can damage data stored on your computer and spread the virus to your computer's other drives or other computers on the network.

There are a vast number of threats that could affect your computer today. This section will go over the threats that Kaspersky Internet Security blocks.

Worms

This malicious program category largely exploits operating system vulnerabilities to spread itself. The class was named for the way the worms crawl from computer to computer, using networks, e-mail, and other data channels. This feature gives many worms a rather high speed in spreading themselves.

Worms penetrate a computer, calculate the network addresses of other computers, and send a burst of self-made copies to these addresses. In addition to network addresses, worms often utilize data from e-mail client address books. Some of these malicious programs occasionally create working files on system disks, but they can run without any system resources at all (with the exception of RAM).

Viruses

Programs that infected other programs, adding their own code to them to gain control of the infected files when they are opened. This simple definition explains the fundamental action performed by a virus – *infection*.

Trojans

Programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang, stealing confidential information, etc. This class of malicious program is not a virus in the traditional sense of the word (meaning it does not infect other computers or data). Trojans cannot break into computers on their own and are spread by hackers, who disguise them as regular software. The damage that they incur can exceed that done by traditional virus attacks by several fold.

Recently, the most widespread type of malicious program damaging computer data has been worms. Then follow viruses and Trojans. Some malicious programs combine features of two or even three of these classes.

Adware

Program code included in software, unbeknownst to the user, designed to display advertisements. Adware is usually built into software that is distributed free. The advertisement is situated in the program interface. These programs often also collect personal data on the user and send it back to their developer, change browser settings (start page and search pages, security levels, etc.) and create traffic that the user cannot control. All this can lead to breach of the security policy and to direct financial losses.

Spyware

Software that collects information about a particular user or organization without their knowledge. You might never guess that you have spyware installed on your computer. In general, the goal of spyware is to:

- trace user actions on a computer;
- gather information on the contents of your hard drive; in such cases, this more often than not involves scanning several directories and the system registry in order to compile a list of the software installed on the computer;
- gather information on the quality of the connection, bandwidth, modem speed, etc.

Riskware

Potentially dangerous software that does not have a malicious function but can be used by hackers as an auxiliary component for a malicious code, since it contains holes and errors. Under certain conditions, having such programs on your computer can put your data at risk. These programs include, for instance, some remote administration utilities, keyboard layout togglers, IRC clients, FTP servers, and all-purpose utilities for stopping process or hiding their operation.

Yet another type of malicious program that goes along with programs like adware, spyware, and riskware is programs that plug into your web browser and redirect traffic. You have most certainly encountered such programs if you have ever opened one web site when you thought you were pulling up another.

Jokes

Software that does not do any direct damage but displays messages stating that damage has already been done or will be under certain conditions. These programs often warn the user of dangers that do not exist, such as messages that pop up about formatting the hard drive (although no formatting actually takes place) or detecting viruses in uninfected files.

Rootkits

Utilities used to conceal malicious activity. They mask malicious programs to keep anti-virus programs from detecting them. Rootkits modify the operating system on the computer and alter its basic functions to hide its own existence and actions that the hacker undertakes on the infected computer.

Other dangerous programs

Programs created to set up DoS attacks on remote servers, hacking into other computers, and programs that are part of the development environment for malicious programs. These programs include hack tools, virus builders, vulnerability scanners, password-cracking programs, and other types of programs for cracking network resources or penetrating a system.

Hacker attacks

Hacker attacks can be initiated by hackers or by malicious programs. They are aimed at stealing information from a remote computer, causing the system to malfunction, or gaining full control of the system's resources.

Some types of online scams

Phishing is an online scam that uses mass mailings to steal confidential information from the user, generally of a financial nature. Phishing e-mails are designed to maximally resemble informative e-mails from banks and well-known companies. These e-mails contain links to fake sites set up by hackers to copy the site of the organization that they claim to represent. On this site, the user is asked to enter, for example, his credit card number and other confidential information.

Dialers to pay-per-use websites – type of online scam using unauthorized use of pay-per-use Internet services (these are commonly web sites of a pornographic nature). The dialers installed by hackers initiate modem connections from your computer to the number for the pay service. These numbers often have very high rates and the user is forced to pay enormous telephone bills.

Intrusive advertising

This includes popup windows and banner ads that open when using your web browser. The information in these windows is generally not of benefit to you. Popup windows and banner ads distract the user from the task and take up bandwidth.

Spam

Spam is anonymous junk e-mail. Spam includes mailings that are marketing, political and provocative in nature and e-mails asking for assistance. Another category of spam includes e-mails that ask one to invest large amounts of money or to get involved in pyramid schemes, e-mails aimed at stealing passwords and credit card numbers, and e-mails that ask to be sent to friends (chain letters).

Henceforth in the text of this User's Guide the term "virus" will be used to refer to malicious software and the term “dangerous objects” will be used to refer to objects infected with such software. A particular type of malware will be mentioned only when it is required.

1.2. The purpose and major functions of Kaspersky Anti-Virus Personal Pro

Kaspersky Anti-Virus Personal Pro (hereinafter referred to as Kaspersky Anti-Virus or the application) is designed to provide anti-virus protection for personal computers running Microsoft Windows (see section 1.4 on page 14).

When installed on your computer, the application performs the following functions:

- **Protection against viruses and malicious computer programs** – the application detects and eradicates malware present in your computer. When using the application, the following two major modes can be used (either jointly or separately):
    - **Real-time anti-virus protection** – performs an anti-virus scan of all objects being run, opened or saved.
    - **On-demand scan** – performs an anti-virus scan of your entire computer or of selected disks, files, or folders. You can launch an on-demand scan manually or set up a regular scheduled scan.
- **Recovery from a virus attack** – performing a full scan and disinfection using settings recommended by Kaspersky Lab will allow you to detect any viruses that have infected your files during a virus attack.
- **Scanning and disinfecting of incoming/outgoing email traffic** – real-time protection performs a real-time anti-virus scan and disinfection of incoming and outgoing email messages1. In addition, the application provides on-demand scanning and disinfection of the email databases of email clients[2] (see section 6.3.3 on page 52).
- **Protection of the user's computer against network attacks** – analysis of all data entering the user's computer from the network (either LAN or internet) to determine whether these data is a part of an internet attack. If an internet attack is detected, the attack will be repelled the attacking computer can be blocked. Additionally, the program provides for the operation in the stealth (invisible) mode when the user's computer receives data from other computers only when the data exchange with the particular machine has been initiated by the user.
- **Updating of the anti-virus database, network attacks database and application modules** – updating the anti-virus database and network attacks database with information about new viruses and attacks and with methods used for disinfecting objects infected with viruses and updating the application modules (if this option is not disabled). Updates are

[1] The application scans all mail sent or received by Microsoft Office Outlook irrespective of the mail protocols used as well as mail sent or received by any mail client application via SMTP and POP3 protocols.

[2] Kaspersky Anti-Virus® can scan email databases for any email client program, but can disinfect only Microsoft Office Outlook and Microsoft Outlook Express email databases.

downloaded from Kaspersky Lab's update servers, server specified by the user or copied from a network/local folder.

- **Recommendations on application setup and operation** – the application will display tips from Kaspersky Lab's experts and recommendations on the settings that correspond to the optimal anti-virus protection level.

  When a dangerous object is found, if the anti-virus database have been not updated for a critically long time, or your computer has not been scanned for a long time, the main window of Kaspersky Anti-Virus will recommend a course of action and give a supporting explanation.

  Kaspersky Lab's experts have configured the application for optimal performance based on the extensive expertise in the anti-virus protection business, and on analysis of our users' feedback. The recommended anti-virus protection settings are installed as the default application settings.

- **Using various application configuration profiles** – creating and using special configuration files (profiles) that store the application's operation settings. You can easily alter the Kaspersky Anti-Virus configuration by specifying the application's settings and saving such changes in the profiles. For example, you can configure the application to work in the real-time protection mode only or to perform on-demand scan and then use such configurations when you feel it is necessary. You can also return to the recommended settings any time while using Kaspersky Anti-Virus.

- **Moving to quarantine** – moving objects that are possibly infected with viruses or their modifications to a special secure storage area. You can then disinfect or delete the quarantined objects, restore them to their initial folders or send them to Kaspersky Lab for analysis. Quarantined files are stored using a special format and do not constitute any danger to your computer.

- **Creating backup copies of objects** – creating backup copies of objects in a special backup storage prior to disinfection or deletion of such objects. Such copies are created for the cases when it is necessary to restore an original object if it contains valuable information or in order to restore the infection situation for analysis purposes. Backup copies are stored in a special format and do not impose any threat.

- **Reporting** – results of all actions performed by Kaspersky Anti-Virus are documented in reports. A detailed scan report contains statistics of all scanned objects, stores information about settings used for each task and the history of actions performed on each individual file. Reports are also generated during real-time protection, and after updating the anti-virus database and application modules.

Some functions of Kaspersky Anti-Virus are available only from the command line (details see Chapter 10 on page 132).

1.3. What's new in Version 5.0?

Kaspersky Anti-Virus Personal Pro 5.0 has the following features not found in Version 4.5:

- *The use of anti-virus scan acceleration technologies iChecker™ and iStreams™*. Version 5.0 does not scan previously analyzed objects that have not changed since their last scan. This applies both to real-time protection and to the on-demand scan. This feature greatly improves the application’s speed and performance.
- Scanning and disinfecting mail sent and received by any email client that via SMTP and POP3 protocol. The previous version protected only mail sent and received by Microsoft Office Outlook.
- *Disinfecting infected archives*. Version 5.0 disinfects infected files in *zip*, *arj*, *cab*, *rar*, *lha* and *ice* archives. The previous version provided detection and disinfection of infected files in zip archives only.

  Kaspersky Anti-Virus only scans multiple volume archives of the specified types as well as self-extracting archives but does not disinfect them.
- *Anti-virus updating function has become faster* due to finding the geographically closest Kaspersky updates server. The ability to receive the remaining part of the update after restoring failed connection has been implemented.
- *Protection against network attacks*. This version of Kaspersky Anti-Virus protects your computer against most network or hacking attacks that are currently widespread.
- *User-friendly interface*. This version is a single application, whereas the previous release consisted of several components each performing their own anti-virus protection function. This new approach simplifies control over the most important Kaspersky Anti-Virus functions.
- *Improved compatibility of Kaspersky Anti-Virus with other anti-virus products.* During the installation of the application you can choose not to enable file system mail and network protection and script monitoring if these protection functions are performed by other applications installed on your computer.

- *Recommended settings and experts' tips*. To simplify application operation, the default settings of this version of the application match the settings recommended by Kaspersky Lab and in most cases there is no need to configure the application before use. When the anti-virus protection level is set to High Speed, the user is prompted to switch to a higher level of anti-virus protection.

- *Application operation profiles management*. A possibility to store the application's settings in a special file so that you can use them any time later. If you are not satisfied with the recommended Kaspersky Anti-Virus settings, configure the application based on your requirements and save this configuration in a profile file.

- *Product license renewal*. Users of Version 5.0 can now install a new license key, extending the license period.

- *Sending your files for analysis to Kaspersky Lab*. Now you can send us possibly infected files detected by Version 5.0 or files that you suspect may be infected.

- *The ability to delete infected composite objects has been removed*. You cannot inadvertently delete infected composite objects (archives, email clients' databases or email format files) using Version 5.0. However, you can still delete such objects using standard Windows tools such as Windows Explorer. The exception is self-extracting archives.

- *The ability to create lists of trusted processes*. The file activities of the trusted processes are not monitored by Kaspersky Anti-Virus when it functions in the real-time protection mode.

- *Access to the Kaspersky Anti-Virus settings is now password-protected*. You can setup a password that will be asked for by the application every time when switching between the user's and the administrator's mode. The user's mode does not allow modification of the application's settings, disabling the real-time protection and closing Kaspersky Anti-Virus Personal Pro on your computer..

1.4. Hardware and software system requirements

For normal performance of Kaspersky Anti-Virus Personal Pro 5.0, your computer must meet the following minimum requirements:

General Requirements:

- 50 MB available space on your hard drive

- CD-ROM drive (for installation of Kaspersky Anti-Virus from CD) or floppy drive (for installation from floppy disks, and to read license key)
- Microsoft Internet Explorer 5.5 or higher (for updating anti-virus database and application modules via the Internet)

Microsoft Windows 98, Microsoft Windows ME, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Intel Pentium 300 MHz processor
- 64 MB RAM

Microsoft Windows ME:

- Intel Pentium 150 MHz processor
- 32 MB RAM

Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Intel Pentium 133 MHz processor
- 32 MB RAM

Microsoft Windows 2000 Professional (Service Pack 2 or later), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 or later):

- Intel Pentium 300 MHz processor
- 128 MB RAM

Microsoft Windows XP Home Edition or XP Professional (Service Pack 1 or later):

- Intel Pentium 300 MHz processor
- 128 MB RAM

1.5. Distribution Kit

You can purchase Kaspersky Anti-Virus either from our dealers (retail box) or online (for example, you may visit http://www.kaspersky.com, and go to **E-Store** section).

The contents of the retail box package include:

- Sealed envelope with an installation CD, or set of floppy disks, containing the application files.
- User's Guide.

- License key written on a special floppy disk.
- License Agreement.

Before you open the envelope with the CD (or a set of floppy disks) make sure that you have carefully read the license agreement.

If you buy Kaspersky Anti-Virus online, you will download the application from the Kaspersky Lab website. In this case, the distribution kit will include this User's Guide along with the application. The license key will be emailed to you upon receipt of your payment.

The License Agreement is a legal contract between you and Kaspersky Lab that describes the terms and conditions under which you may use the anti-virus product that you have purchased.

Please read the License Agreement carefully!

If you do not agree with the terms and conditions of the License Agreement, return the retail box to the Kaspersky Anti-Virus dealer you purchased it from and the money you paid for the product will be refunded to you on the condition that the envelope with the installation CD (or set of floppy disks) is still sealed.

By opening the sealed envelope with the installation CD (or set of floppy disks), you confirm that you agree with all the terms and conditions of the License Agreement.

1.6. Services provided for registered users

Kaspersky Lab offers all registered users an extensive service package enabling them to use Kaspersky Anti-Virus more efficiently.

After purchasing a license you become a registered user and during the license period you can enjoy the following services:

- application module and anti-virus database updates;
- support on issues related to the installation, configuration and use of the application. Services will be provided by phone or via email;
- information about new Kaspersky Lab products. You can also subscribe to the Kaspersky Lab newsletter which provides information about new computer viruses as they appear.

Kaspersky Lab does not provide support on issues related to the performance and the use of operating systems or other technologies.

1.7. Conventions

In this book we use various conventions to emphasize different meaningful parts of the documentation. The table below lists the conventions used in this document.

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.
Note	Additional information, notes.
Attention	Critical information.
To run a program: Step 1. …	Actions that must be taken to run a program.
Task:	Task statement as an example of parameter definitions, functions, etc.
Solution	Solution to the task formulated.

CHAPTER 2. INSTALLING THE APPLICATION

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

Installation of the application using the distribution kit downloaded from the internet is identical to the installation from the distribution kit on CD.

The installation wizard operates in an interactive mode. Each dialog box has the following buttons that you can use to navigate through the installation process:

- **Next>** – accept and proceed with the installation.
- **<Back** – return to the previous stage of the installation process.
- **Cancel** – cancel the application installation.
- **Finish** – finish the application installation.

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

Step 1. Checking the version of the operating system installed on your computer

Before the installation of the application, the operating system and Service Packs installed on your computer are checked for the conformity with the minimum system requirements for the installation of Kaspersky Anti-Virus Personal Pro.

Should the application determine that any of the requirements is not met, the corresponding message will be displayed. We advise to install the required programs and update packages of Microsoft Windows using **Windows Update** (or other utilities) or before proceeding with the installation of Kaspersky Anti-Virus.

Step 2. Search for other anti-virus software

The next step involves a search for other installed anti-virus software (including Kaspersky Lab applications). This is performed because the simultaneous use of these applications with Kaspersky Anti-Virus may cause conflicts.

If an earlier version of Kaspersky Anti-Virus is found (as for example version 4.5), you will be asked if you would like to keep the license key for this product if such license key is still valid.

We recommend that you keep the valid license key that was used earlier as this key can be used with Kaspersky Anti-Virus Personal Pro 5.0.

After you save the key, you will be prompted to uninstall the earlier version of the product as it is in conflict with Kaspersky Anti-Virus Personal Pro 5.0.

Click **OK** button in order to abort the installation. After this uninstall the earlier version of Kaspersky Anti-Virus and run the product installation wizard again.

If during the previous step you saved a valid license key used for Kaspersky Anti-Virus 4.x to be used in version 5.0, then the license key installation window will not be displayed during the installation procedure (see Step 8. on page 21). The key will be used for the program operation.

If any anti-virus software from a different vendor is found installed on your computer, you will be prompted to uninstall this program before proceeding with the installation of Kaspersky Anti-Virus.

We recommend that you uninstall such program(s). To do this, click the **No** button, in order to abort the installation. Then uninstall the program and run the product installation wizard again.

Kaspersky Lab's specialists do not recommend installing several anti-virus products on one computer as their joint use may cause conflicts.

If it is determined that Kaspersky Anti-Virus Personal Pro 5.0 has already been installed on your computer, a message will be displayed with a warning that if you proceed with the installation, the application that was installed earlier will be updated by the new installation.

If you are upgrading version 5.0, the license key installation window (see Step 8. on page 21) will not contain information about they key, but the key installed earlier will be used for the program operation.

Step 3. Start the Installation Wizard

If no other anti-virus software is found installed on your computer, immediately after the executable file is run, an installation startup window will appear to inform you that the installation of Kaspersky Anti-Virus Personal Pro on your computer began.

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

Step 4. Read the license agreement

The next dialog box contains a License Agreement between you and Kaspersky Lab. Read it carefully and click **I Agree** if you agree with all terms and conditions of the Agreement. The installation process will continue.

Step 5. Provide user information

At this point the user name and the user's company name will be determined. Default information will be copied from the operating system registry. You can alter it if you wish.

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

Step 6. Read important information about the application

During this stage of the installation process you will be asked to read important information about the application before you start using Kaspersky Anti-Virus.

This dialog box contains information about the major features and functionality of Kaspersky Anti-Virus.

In order to proceed to the next step of the setup process, click **Next >**.

Step 7. Using the proprietary Kaspersky Lab's technology

During this step of the Kaspersky Anti-Virus setup process you will have to make a decision whether you want the program to use the following technologies:

Real-time file system protection – scanning all objects that are run, opened and saved on your computer for viruses. By default the file protection is enabled. If you do not want Kaspersky Anti-Virus to scan files when you access them, uncheck the ☑ **Use real-time file system protection** box.

Real-time mail protection – scanning all messages received by your computer, messages you send and your mail databases for viruses. By default mail protection is enabled. If you do not want Kaspersky Anti-Virus to scan mail messages for viruses, uncheck the ☑ **Use real-time mail protection** box.

Monitoring of executed scripts – anti-virus analysis of all VBScripts and JavaScripts before their execution. By default script monitoring function is enabled. If you do not wish to use Kaspersky Anti-Virus for script monitoring, uncheck the ☑ **Use script monitoring** box.

Macros monitoring – scanning all VBA macros run on your computer for the presence of malicious code. By default this protection is enabled. In order to disable macros monitoring, uncheck the ☑ **Use macros monitoring** box.

Real-time protection against network attacks – technology used to protect your computer against hackers attacks. This technology protects your computer against network attacks and prevents corruption, theft of or unauthorized access to your data. By default the real-time protection against network attacks is enabled. In order to disable real-time protection, uncheck the ☑ **Use real-time protection against network attacks** box.

iStreams™ Technology – an anti-virus scan acceleration technology (details see Appendix B on page 151). In order to disable this technology uncheck the ☑ **Use the iStreams™ technology** checkbox.

This technology can only be used on partitions with the NTFS file system.

If you disable the use of the above technologies during the installation, you will have to run the installer again and select technologies that you would like to use.

If, while working with Kaspersky Anti-Virus, you decide to disable one of the real-protection types or to disable Streams™ technology you will have to run the installer again and uncheck the corresponding box.

In order to proceed with the setup process, press **Next>**.

Step 8. Install the license key

Perform this step only if the Kaspersky Anti-Virus Installation Wizard fails to find the key file automatically

During this step, the license key for Kaspersky Anti-Virus will be installed. The license key is your personal "key" that stores all service information required for proper full-featured operation of the application, including the following reference information:

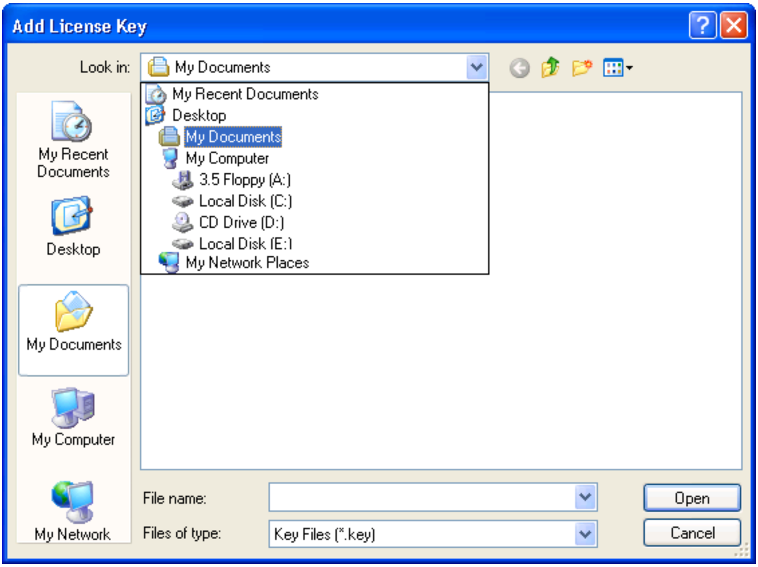
- Technical support information (support service provider and contact information).
- License name, number, and expiry date.

The application will not work without the license key.

In order to install a license key,

1. Press the **Browse** button and browse to the folder containing the license key file:

   - If you purchased a retail box version of Kaspersky Anti-Virus, you will find the license key written or a special floppy disk. You will have to insert the disk into the drive and select this drive (see Figure 1).



Add License Key

Look in: My Documents

File name:

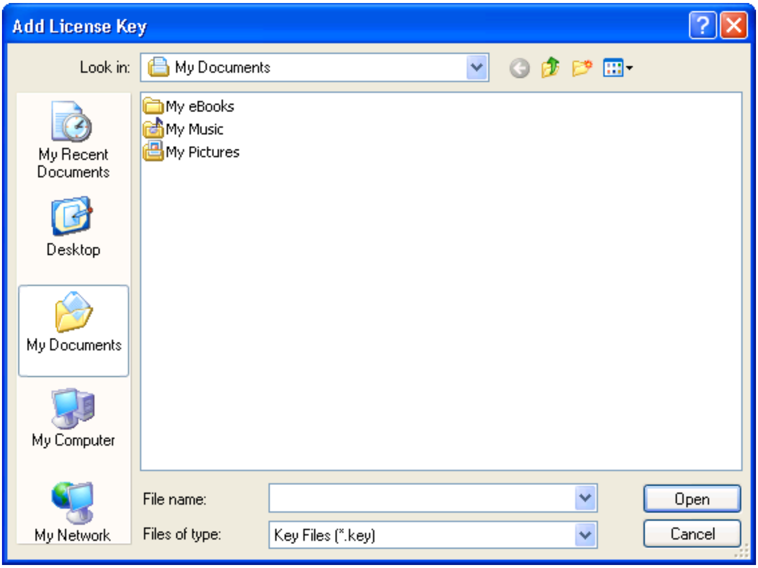
Files of type: Key Files (*.key)

Figure 1. Selecting path to the license key file

   - If the license was purchased online, then the license key file that you received by via e-mail shall be saved in any folder on your computer's hard drive. You will have to open this folder.

   The selected folder will display the list of available license keys.

2. Select the required license key (a file with **.key** extension) and press the **Open** button (see Figure 2).



Add License Key

Look in: My Documents

My eBooks
My Music
My Pictures

File name:

Files of type: Key Files (*.key)

Figure 2. Selecting the license key file

As the result, the installation wizard will display general information about the license and the path to the license key file.

In order to proceed with the installation press **Next >**.

If you do not have the license key at the time of installation (for example, if you ordered via the Internet but have not received it yet), you may install it later, when you run the application for the first time or using a special license key installation utility (see Chapter 9 on page 128). Remember that you cannot start using Kaspersky Anti-Virus without the license key.

Step 9. Select the installation folder

During this step, the destination folder will be selected for the installation of the application files. The default path is: **<Disk>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus Personal Pro**.

You can type in the path to this folder or press the **Browse** button and use the standard **Select Folder** dialog box to locate and select the folder.

Press the **Install** button in order to proceed with the installation. After this, Kaspersky Anti-Virus application files will be copied to your computer.

Step 10. Finish setup

A **Completing the Setup** dialog box informs you that installation of Kaspersky Anti-Virus on your computer has been completed.

If registration of system services is required, you will be asked to restart your computer. This is a MANDATORY step for the correct completion of the application installation.

To complete the setup:

1. Choose one of the following options:

   ● **Yes, I want to restart my computer now**

   ● **No, I will restart my computer later**

2. Click **Finish**.

If your computer does not need to be restarted to complete the setup, you can begin using the program immediately. Perform the following steps to finish the installation:

1. If you do not want to enable anti-virus protection of your computer immediately after the installation is completed, uncheck the box ☑ **Start Kaspersky Anti-Virus Personal Pro 5.0**.

   If you uncheck this box, the anti-virus protection of your computer will be automatically enabled after reboot. Before that time you can manually enable anti-virus protection from the Microsoft Windows main menu (**Start → Programs → Kaspersky Anti-Virus Personal Pro**).

2. Click the **Finish** button.

As a result of installation and launch of Kaspersky Anti-Virus:

- The application icon will be added to the system tray
- Application shortcuts will be added to the main Microsoft Windows menu (**Start→ Programs→ Kaspersky Anti-Virus Personal Pro**).

CHAPTER 3. PREVENTING COMPUTER INFECTION

Sometimes it is not apparent, even to a knowledgeable user, that a computer is infected with a virus because viruses efficiently camouflage themselves among regular files. This chapter contains a detailed discussion of virus infection symptoms, methods of data recovery after a virus attack and measures aimed at prevention of data corruption by viruses.

3.1. Symptoms of infection

There are a number of symptoms indicating that your computer has probably been infected. If you are noticing "strange things" happening to your computer, for example:

- unexpected messages or images are suddenly displayed;
- unusual sounds or music played at random;
- your CD-ROM tray mysteriously opens and closes;
- programs suddenly start on your computer;
- if Kaspersky Anti-Hacker is installed on your computer, it notifies you of attempts by some programs to connect to the Internet although you did not initiate this.

If any of the above symptoms appear, it is very likely your computer has been infected with a virus.

In addition, there are some typical symptoms indicating that your computer has been infected via email:

- your friends mention that they receive messages although you never sent such messages;
- your mailbox contains many messages without the sender’s email address or header.

Note that these problems may be caused by reasons other than viruses. For example, infected messages which have your address as the sender can actually be sent from a different computer.

There are also indirect symptoms that indicate your computer has possibly been infected:

- your computer freezes frequently or encounters errors;
- your computer slows down when programs are started;
- you are unable to load the operating system;
- files and folders are suddenly missing or their content changes;
- your hard drive is accessed too often (the light on your main unit flashes rapidly);
- Microsoft Internet Explorer "freezes" or displays unpredictable behavior, (for example you cannot close the application window).

In most cases such indirect symptoms indicate that there is a hardware or software problem, but although such symptoms are unlikely to be caused by an infection, we recommend that you perform a full scan of your computer using the default settings recommended by Kaspersky Lab experts if your encounter any of these problems.

3.2. What should you do if you notice symptoms of infection

If you notice that your computer displays "suspicious" behavior:

1. Don’t panic! This golden rule may prevent the loss of important data stored on your computer and help you avoid unnecessary stress.
2. Disconnect your computer from the Internet.
3. Disconnect your computer from the Local Area Network if it is con
4. If the symptom of an infection is that you cannot boot from your hard drive (your computer encounters an error at startup), try to start the system in Safe Mode or from the Microsoft Windows boot disk that you created during the installation of the operating system on your computer.
5. Before taking any action, back up all critical data to an external drive (a floppy disk, CD, flash card, etc.)

Later, before you move saved date to the computer after it has been disinfected, make sure that you have scanned this data with Kaspersky Anti-Virus (see section 6.3.5 on page 57).

6. Install Kaspersky Anti-Virus Personal Pro.
7. Download the latest anti-virus database updates. If possible, do not use the infected computer to download the updates, but instead use a friend's computer, or a computer at your office or an Internet café. It is preferred that you use a different computer because when you connect to the internet using an infected computer some important information stored on your computer may be sent to the malefactors or the virus may be sent to the contacts stored in your address book. Therefore, if you suspect an infection it is the best to immediately disconnect from the Internet and from any local area network you are connected to. You can also obtain the anti-virus database on a CD-ROM or a floppy disk from Kaspersky Lab or its authorized dealers and update your databases from this disk (for more details see section 7.1.1 on page 63).
8. Apply the recommended application settings (see Chapter 4 on page 30).
9. Perform a full system scan (see section 6.3.2 on page 51).

3.3. Safety rules

Even proven and trusted preventative actions cannot ensure 100% protection against computer viruses and Trojans, but you can considerably minimize the risk of being affected by a virus attack and thus reduce the losses from a possible infection if you develop and follow certain rules.

Similar to health care, one of the main methods of fighting viruses is the *prevention* of infection. For computers, prevention of a virus infection includes a few rules that must be followed to reduce the risk of infection and data loss.

Listed below are the main security rules that you should follow to prevent virus attacks.

Rule 1: keep your computer protected with an anti-virus program and Internet security software. To do this:

- Install Kaspersky Anti-Virus Personal Pro.
- Update your anti-virus database on a regular basis. During periods of virus outbreaks you should retrieve updates several times each day because during such periods the anti-virus database on Kaspersky Lab's update servers is updated constantly.

- Apply the real-time protection settings recommended by Kaspersky Lab. Real-time protection is enabled immediately after system startup and prevents the penetration of viruses into your computer.
- Apply the on-demand scan settings recommended by Kaspersky Lab and schedule the scan to be run at least once a week.
- We also recommend that you install Kaspersky Anti-Hacker for comprehensive computer protection while you are surfing the Internet.

Rule 2: *b*e careful when copying any new data to your computer:

- Always scan all removable drives (floppy disks, CD-ROM drives, flash cards, etc.) for viruses before using them.
- Be careful with email messages. Never open an email attachment, even if it was sent to you by a person you know, unless you are expecting it. In particular, do not trust emails that claim to be sent by anti-virus companies.
- Be careful with any data downloaded from the Internet. If you are prompted to download a program, always check that it comes with a security certificate.
- If you download an executable file from the Internet or from a LAN, scan it with Kaspersky Anti-Virus.
- Be selective about the websites you visit. Some websites contain dangerous scripts or Internet worms.

Rule 3: Read carefully all information supplied by Kaspersky Lab.

In most cases, Kaspersky Lab warns users about new virus outbreaks long before they reach their peak. The risk of getting infected is still low at this time and if you download the up-to-date anti-virus database, you will be able to protect your computer.

Rule 4: *Be suspicious about hoax virus warnings* - email messages that claim to be warnings of virus threats.

Rule 5: Regularly update your operating system using the Microsoft Windows Update utility.

Rule 6: Always buy licensed copies of your software from authorized dealers*.*

Rule 7: Limit the number of people who have access to your computer.

Rule 8: Minimize potential losses from a possible infection:

- Backup your data on a regular basis, so that in the event of data loss, your system may be fairly quickly restored using backup copies. Your distribution disks, floppy disks and other media with software installation and other important data should be kept in a safe place.

- Always create a bootable rescue disk from which you can boot using a "clean" operating system.

Rule 9: *Inspect the list of applications installed on your computer on a regular basis*.

You can access this list using the **Add/Remove programs** utility in the **Control Panel** or simply view the contents of the **Program Files** folder, startup folder. This way you can detect software that was installed onto your computer without your knowledge while you were using Internet or installing some software you needed. There is a very high chance that some of these programs are riskware.

CHAPTER 4. ANTI-VIRUS PROTECTION USING KASPERSKY ANTI-VIRUS DEFAULT SETTINGS

⚠ Real-time protection of your computer is provided only if you did not disable it during the installation of the application.

You can use Kaspersky Anti-Virus immediately upon installation. There is no need to customize the application before using it for the first time because the default settings provide the optimal balance between protection and performance.

Below, we describe the default settings in detail.

According to the default settings, the anti-virus protection becomes active immediately after the application is installed on your computer. The default settings are recommended by Kaspersky Lab's experts to ensure the optimal protection of your computer.

Additionally, the application includes a tool for quick altering the settings by selecting one of the three protection levels, pre-defined by the Kaspersky Lab's experts.

- **Maximum protection** – computer protection level that ensures maximum possible protection with some decrease in the system performance.
- **Recommended** – second anti-virus protection level based on the settings recommended by Kaspersky Lab's experts that ensure optimal protection of your computer.
- **High speed** – anti–virus protection level that ensures maximum speed of operation with somewhat lower extent of the anti-virus protection due to some reduction in the number of scanned objects.

Following below is a detailed discussion of how Kaspersky Anti-Virus performs in accordance with the experts' recommendations.

4.1. Real-Time Protection

Real-time protection is enabled from the moment your operating system has started until you turn off your computer. This is indicated by the red icon in the system tray.

Immediately after the system is started, Kaspersky Anti-Virus scans *its own application modules, RAM, all automatic startup objects* and performs the scan of objects being opened, saved or run in the real-time mode.

By default the real-time protection uses settings recommended by the Kaspersky Lab's experts, namely:

- Objects being opened, saved or executed on your hard drives, network and removable drives that are potentially infectable will be scanned, including:
  - *disk boot sectors* (these objects are scanned immediately after the system startup);
  - *packed files* and objects linked to or embedded into files *(OLE objects);*
  - incoming email messages.

Real-time protection does not scan objects that cannot contain viruses.

- When an *infected* object is detected, the application denies access to this object and prompts the user for action.
- When an object possibly infected with a virus or a virus modification is detected, the application blocks access to it and prompts the user for action.
- When a *network attack* is detected, the application displays a corresponding message, blocks the attack.
- The results of all application actions are documented in reports (see section 8.4 on page 114).

The table below contains information on all possible parameters of the anti-virus file scan. The plus sign ("+") means that this parameter is used a the particular level, and the minus sign ("-") means that this parameter is not used.

	Maximum protection	Recommended	High speed
Protection level	Potentially infectable objects	Potentially infectable objects	Files by extension
Hard drives	+	+	+
Removable drives	+	+	+
Network drives	+	+	-
OLE objects	+	+	-
Packed executable files	+	+	+
Self-extracting archives[3]	+	-	-
Disk boot sectors	+	+	+
Maximum object scanning time (sec.)	-	-	-
Incoming mail (POP3)	+	+	+
Incoming mail (Microsoft Office Outlook)	+	+	+
Outgoing mail (SMTP)	+	-	-
Outgoing mail (Microsoft Office Outlook)	+	-	-
Attached archives	+	+	-
Attached mail databases	+	+	-
Use iStreams™	+	+	+
Use iChecker™	+	+	+

4.2. On-Demand Scan

By default on-demand scan is performed based on the settings recommended by Kaspersky Lab’s experts.

[3] Self-extracting archives will be scanned only within the executable area.

- an on-demand scan of your entire system will scan *RAM used for the running processes* and <u>all objects stored on hard drives</u>, including:
  - *startup objects and disk boot sectors;*
  - *archives, packed executable files and self-extracting archives;*
  - objects linked to or embedded into files (*OLE objects)*;

  ⚠ The full computer scan does not include the analysis of mailboxes that are currently in use.

- an anti-virus scan of a particular disk, folder or file will scan all files located within the selected area, including:
  - *archives*, *packed executable files* and *self-extracting archives*;
  - objects linked or embedded into files (*OLE objects*);
- detected dangerous objects are processed after the scan is complete; possible actions will be listed for each object;
- the results of all application actions are documented in reports (see section 8.4 on page 114).

By default, a full on-demand scan of your computer is scheduled every Friday at 8 pm. The full scan status indicator (see Figure 5) is located in the right section of the **Protection** tab.

✓ **The full scan of your computer is in progress**

If your computer is off at the scheduled time, the scan will not be performed.

The table below contains information on all possible parameters of the anti-virus file scan. The plus sign ("+”) means that this parameter is used a the particular level, and the minus sign (“-“) means that this parameter is not used.

	Maximum protection	**Recommended**	**High speed**
Protection level	Scan objects irrespective of type and extension	Scan objects irrespective of type and extension	Potentially infectable objects
Archives	+	+	-
OLE objects	+	+	+
Packed executable files	+	+	+

	Maximum protection	Recommended	High speed
Self-extracting archives[4]	+	+	+
NTFS-streams	+	+	+
Mail format files	+	-	-
Mail databases	+	-	-
Maximum size of scanned object (KB)	-	-	8192
Maximum object scanning time (sec.)	-	-	60
Prompting for password during the scan	+	-	-
Use iStreams™	+	+	+
Use iChecker™	+	+	+

4.3. Updating the anti-virus database

By default, database updates are automatically downloaded from the Kaspersky Lab's update servers and installed on your computer every 3 hours. If you use your computer less than three hours a day, the anti-virus database will be updated immediately after Kaspersky Anti-Virus is launched.

[4] Self-extracting archives will be scanned only within the executable area.

CHAPTER 5. APPLICATION INTERFACE

Kaspersky Anti-Virus has a simple and easy-to-use interface. In this chapter the main elements of the application interface are discussed: the system tray icon, shortcut menu, main application window and the service windows.

5.1. System Tray Icon

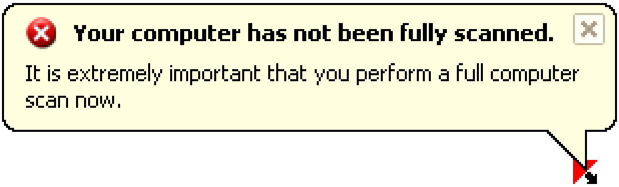
After the application has started, an icon indicating the status of real-time protection will appear in the Windows system tray.

If the application icon is enabled (red color) , this means that all files on your computer are monitored by Kaspersky Anti-Virus. If the icon is disabled (grey color) , is disabled (for example, if you have temporarily or permanently disabled real-time file protection or disabled it during the installation).

When the application is analyzing an object, the lower right-hand corner of the icon becomes a flashing white-and-blue folder: or . When mail is being scanned, an envelope will be displayed instead of the folder - . When the updates are being downloaded, icon will be displayed.

If the system tray icon animation is disabled in Kaspersky Anti-Virus settings (see section 8.6 on page 120), the icon will only have to states: enabled or disabled.

When an important anti-virus event occurs, the recommended action will be indicated in a pop-up window above the icon (see Figure 3). (The information messages are not displayed if you are running Microsoft Windows 98/NT OS)



Your computer has not been fully scanned.

It is extremely important that you perform a full computer scan now.

Figure 3. Information message

5.2. Shortcut menu

To open a shortcut menu, right-click the application icon in the system tray (see Figure 4). The menu includes the following items:

- **Open Kaspersky Anti-Virus** – open the main application window with the **Protection** tab active. You can also open the main window by clicking the K icon in the system tray.
- **Switch to user mode/Switch to administrator mode** – switch from one security mode to another
- **Started tasks** – the list of tasks executed according to the schedule. This menu item appears in the shortcut menu at the moment when a certain task is in progress.
- **Scan My Computer for viruses** – perform a full scan of your computer for viruses using the selected protection level settings.
- **Update Anti-Virus Database** – update the anti-virus database from the updates source specified by the user.
- **Resume/Stop Real-Time Protection** – enable or temporarily disable real-time protection of your computer. This item will only be shown in the application shortcut menu if you did not disable the use of real-time file protection during the installation of Kaspersky Anti-Virus Personal Pro. The application icon in the system tray changes color depending on whether real-time protection is disabled or enabled.

  ⚠ We do not recommend that you stop real-time anti-virus protection because this considerably increases the risk of virus infection of your computer.

- **About** – display general information about Kaspersky Anti-Virus Personal Pro.
- **Exit** – close Kaspersky Anti-Virus and unload it from your computer's memory.

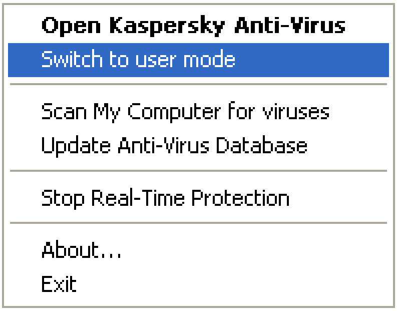

Open Kaspersky Anti-Virus
Switch to user mode
Scan My Computer for viruses
Update Anti-Virus Database
Stop Real-Time Protection
About...
Exit

Figure 4. Shortcut menu

5.3. Main application window: general structure

The main application window gives quick access to all the application's anti-virus protection capabilities. From the main application window, you can perform the following functions:

- start and stop a scan of the entire system or specified disks, folders or files for viruses;
- create your own scanning tasks;
- download updates for the anti-virus database, network attacks database and application modules;
- configure anti-virus protection parameters;
- manage quarantined objects;
- manage object copies created in the backup storage before the attempt to disinfect or delete such objects;
- manage reports, etc.;
- manage the application's configuration, etc.

All anti-virus protection settings, status information and specific tasks are accessible from the following tabs of the main window:

- **Protection** tab – a main window tab that displays the anti-virus protection tasks (objects scan and anti-virus database updating) and their status. From this tab you can switch to quarantine, backup storage and reports. This tab will always open first when you start using the application (see section 5.3.1 on page 39).

- **Settings** tab – a tab that displays the settings and status for all anti-virus tasks (see section 5.3.2 on page 40).
- **Support** tab – a tab where you can view information about the license key, renew the application license, access online Help system and send questions to the Support Service (see section 5.3.3 on page 41).

Each tab has two sections as follows:

- The left section displays links used to control the performance of anti-virus protection tasks. Each tab has its own list of specific tasks.

  For example, the **Protection** tab lists all created anti-virus scan tasks. The **Settings** tab includes hyperlinks used to configure tasks' parameters. The **Support** tab includes tasks that support your anti-virus protection.

- The right section contains information on the current status of the anti-virus protection of your computer, including real-time protection, on-demand scan, anti-virus database and license information.

  Thus, for instance, the **Protection** tab displays the status of your anti-virus protection, the **Settings** tab displays the status of the current application settings and the Support tab displays the license status (license key information), support contact information and information about the application and your system.

Four states of anti-virus protection are indicated in the **Protection** and the **Settings** tabs by the following icons:

✖ *Critical level of anti-virus protection*. This status means that the real-time protection is disabled or that certain tasks (scanning and/or updating) have not been performed for a long time or that the current settings do not provide reliable anti-virus protection of your computer or that an anti-virus task resulted in a failure.

⏸ *Anti-virus protection* is stopped*.* This status indicates that the protection of your computer is temporarily disabled.

⚠ *Anti-virus protection level does not match the recommended settings*. This status indicates that current anti-virus protection settings do not match the recommended settings or that a certain anti-virus protection task must be performed.

✓ The anti-virus protection level is set to Recommended. This status indicates that your settings fully comply with the settings recommended by Kaspersky Lab.

The status information is displayed in the following order: the real-time protection status will be displayed first, the on-demand scan status, and, finally, the status of the anti-virus database validity.

Each state described above is provided with comments and recommendations. Thus, for example, if the current anti-virus protection level does not match the recommended level, you will be prompted to restore the recommended settings to ensure the optimal protection level.

5.3.1. Protection tab

Using the **Protection** tab (see Figure 5), you can scan your entire computer or individual disks, folders or files. You can also:

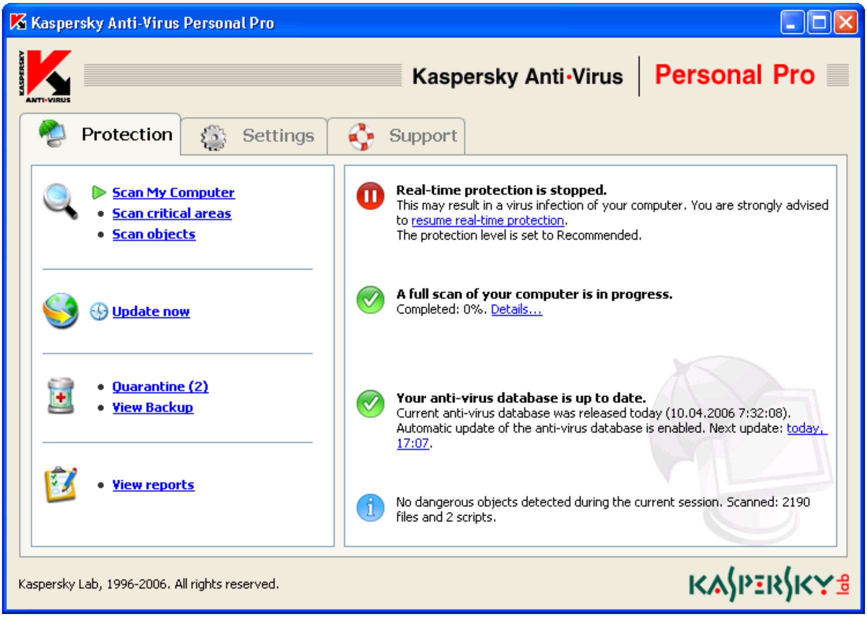
- launch the updating of the anti-virus database, application modules and network attacks database;
- switch to progress reports on all running tasks (view, delete, export to a file).
- switch to managing quarantined objects that are possibly infected with a virus or a virus modification.
- switch to managing backup copies of disinfected or deleted objects

These tasks can be launched by clicking the corresponding links.

In the right section of the tab, you can view the current status of real-time protection, full computer scan and anti-virus database. For example, on Figure 5 you can see that real-time protection is stopped and a full scan is now being performed. Here you can also view comments on the status of each anti-virus protection task.

If the protection status is critical or does not match the recommended settings, you will be prompted to modify the current settings, restore the recommended settings, or launch a certain task. The recommendations are organized as hyperlinks so that you can easily perform the corresponding action.

You can review the application’s performance statistics in the lower part of the **Protection** tab. The information includes the total number of objects scanned during the current session and the number of dangerous objects detected.



Real-time protection is stopped.
This may result in a virus infection of your computer. You are strongly advised to resume real-time protection.
The protection level is set to Recommended.

A full scan of your computer is in progress.
Completed: 0%. Details...

Your anti-virus database is up to date.
Current anti-virus database was released today (10.04.2006 7:32:08).
Automatic update of the anti-virus database is enabled. Next update: today, 17:07.

No dangerous objects detected during the current session. Scanned: 2190 files and 2 scripts.

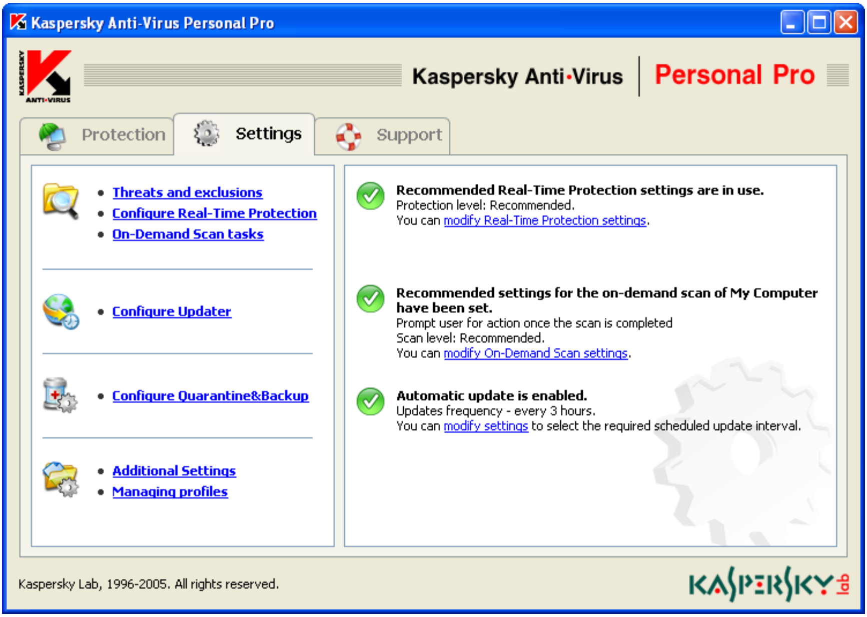
Kaspersky Lab, 1996-2006. All rights reserved.

Figure 5. **Protection** tab

5.3.2. *Settings* tab

Using the **Settings** tab (see Figure 6) you can evaluate and customize both the standard and advanced settings to ensure smooth performance of Kaspersky Anti-Virus.

The right section of the tab displays the current settings for real-time anti-virus protection, on-demand full computer scans, and automatic updating of the anti-virus database, application modules and the known network attacks database. It also gives detailed comments and tips from Kaspersky Lab on how to customize these settings. For example, if you updated your anti-virus database manually in the past, you will be prompted to schedule automatic updates.


Kaspersky Anti-Virus Personal Pro
Kaspersky Anti-Virus | Personal Pro
Protection
Settings
Support

- Threats and exclusions
- Configure Real-Time Protection
- On-Demand Scan tasks

- Configure Updater

- Configure Quarantine&Backup

- Additional Settings
- Managing profiles

Recommended Real-Time Protection settings are in use.
Protection level: Recommended.
You can modify Real-Time Protection settings.

Recommended settings for the on-demand scan of My Computer have been set.
Prompt user for action once the scan is completed
Scan level: Recommended.
You can modify On-Demand Scan settings.

Automatic update is enabled.
Updates frequency - every 3 hours.
You can modify settings to select the required scheduled update interval.

Kaspersky Lab, 1996-2005. All rights reserved.

Figure 6. The **Settings** tab

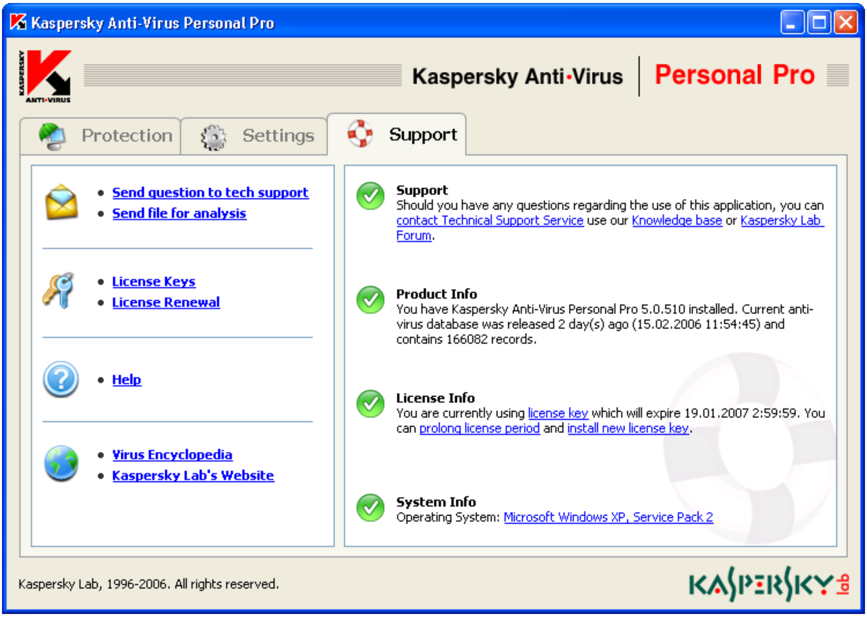
By clicking links located in the left section of the **Settings** tab, you can edit the parameters for real-time protection, on-demand scans and updating. You can also create the list of objects that will be excluded from the scan scope and specify the type of the anti-virus database used.

Here you can also customize parameters related to the quarantine where suspicious objects are placed as well as the parameters of the backup storage used to keep backup copies of objects. Finally you can customize additional settings by following the link Additional Settings.

Kaspersky Anti-Virus offers a possibility to the user to create various working configurations and save them into special configuration files called *profiles*. Later you can easily return to the configuration you need by simply loading the required profile without the need to configure the application manually. You can switch to creating and loading profiles using the Managing profiles hyperlink.

5.3.3. *Support* tab

The **Support** tab (see Figure 7) displays contact information for Kaspersky Lab's Technical Support and how to obtain assistance for problems with Kaspersky Anti-Virus operation. The right section of the tab displays information about the application, the license key and the computer's operating system so that you can provide this information to Technical Support if required.



Support
Should you have any questions regarding the use of this application, you can contact Technical Support Service use our Knowledge base or Kaspersky Lab Forum.

Product Info
You have Kaspersky Anti-Virus Personal Pro 5.0.510 installed. Current anti-virus database was released 2 day(s) ago (15.02.2006 11:54:45) and contains 166082 records.

License Info
You are currently using license key which will expire 19.01.2007 2:59:59. You can prolong license period and install new license key.

System Info
Operating System: Microsoft Windows XP, Service Pack 2

Kaspersky Lab, 1996-2006. All rights reserved.

Figure 7. The **Support** tab

By following the links in the left section of the tab, you can:

- send your questions and objects possibly infected with viruses or their modifications to Kaspersky Lab's Technical Support;
- renew the license for Kaspersky Anti-Virus Personal Pro.

The left section of the tab also includes the following reference hyperlinks:

- Help – general application reference.
- Virus Encyclopedia – a hyperlink to www.viruslist.com website that contains detailed description of all currently known malware.
- Kaspersky Lab's Website – a hyperlink to the Kaspersky Lab's website.

5.4. Scan window

After you launch an anti-virus scan of all or part of your computer, the scan window will appear (see Figure 8).

The scan window consists of two parts:

- the top part of the window contains a scan progress bar showing the percentage of scan progress, the name of the object currently scan, the estimated time of the scan completion and the general statistical data about the objects scanned, disinfected, removed and quarantined so far.

- the bottom part of the window opens by clicking the ▼ button. It contains three tabs: **Statistics**, which displays the scan results; **Report**, which contains a report on the events that occurred during the scan; and **Settings**, which contains a list of settings used for the current scan or for the last scan performed. You can then hide the bottom part by clicking the ▲ button.

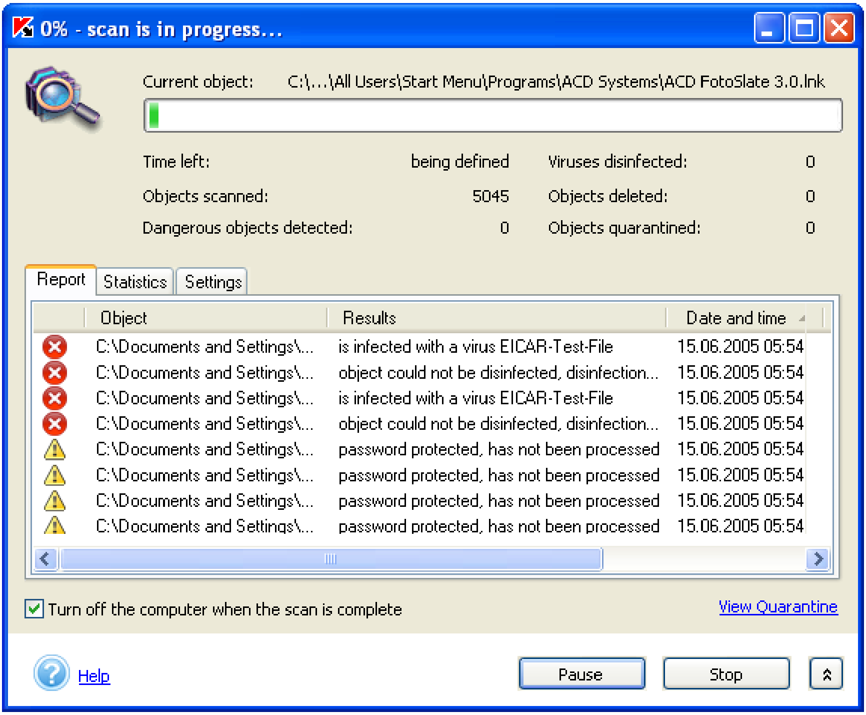
See section 8.4 on page 114 for report details.

You can switch to the quarantine storage window by following the View quarantine link (see section 8.2 on page 110).

If you perform a full computer scan, then using this window you can enable the automatic computer turn-off after the scan is complete. This mode is convenient if you start the computer scan at the end of your business day and do not want to wait until the scan is complete to turn off your computer manually.

However, this mode requires the following additional preparation: before you launch the scan you will have to disable prompting for password when scanning objects (if it is enabled) (see section 7.3.2.1 on page 92), setup the automatic processing mode for dangerous objects, their deletion, quarantining or recording information about them into the reports (see section 7.3.2.2 on page 95). These actions will disable the interactive mode of the program operation and the program will not prompt you for answers that interrupt the scanning process.

In order to automatically turn-off your computer after the scan is complete, check the ☑ **Turn-off the computer when the scan is complete** checkbox in the scan window.



0% - scan is in progress...

Current object: C:\...\All Users\Start Menu\Programs\ACD Systems\ACD FotoSlate 3.0.lnk

Time left:	being defined	Viruses disinfected:	0
Objects scanned:	5045	Objects deleted:	0
Dangerous objects detected:	0	Objects quarantined:	0

	Object	Results	Date and time
✖	C:\Documents and Settings\...	is infected with a virus EICAR-Test-File	15.06.2005 05:54
✖	C:\Documents and Settings\...	object could not be disinfected, disinfection...	15.06.2005 05:54
✖	C:\Documents and Settings\...	is infected with a virus EICAR-Test-File	15.06.2005 05:54
✖	C:\Documents and Settings\...	object could not be disinfected, disinfection...	15.06.2005 05:54
⚠	C:\Documents and Settings\...	password protected, has not been processed	15.06.2005 05:54
⚠	C:\Documents and Settings\...	password protected, has not been processed	15.06.2005 05:54
⚠	C:\Documents and Settings\...	password protected, has not been processed	15.06.2005 05:54
⚠	C:\Documents and Settings\...	password protected, has not been processed	15.06.2005 05:54

☑ Turn off the computer when the scan is complete

Figure 8. The **Scan** window

5.5. Application reference system

Comprehensive application reference information is available from the **Support** tab of the main application window by simply following the Help link in the left section of the tab.

If you have a question on a particular dialog box, press the **<F1>** key or click Help in the left bottom corner of this dialog box.

CHAPTER 6. USING THE APPLICATION

6.1. Updating the anti-virus database

Kaspersky Lab provides the possibility for its users to update the Kaspersky Anti-Virus Personal Pro application modules, the anti-virus database used by the application to detect malicious software and to disinfect infected objects as well as the network attacks database that is used to protect the user against such attacks.

Timely updating of the anti-virus database ensures the safety of your computer. Dozens new viruses appear daily, and in response Kaspersky Anti-Virus experts update our anti-virus database with the latest information about these new threats. We recommend that you update your anti-virus database at least once every 3 hours; during periods of virus outbreaks the anti-virus database should be updated as frequently as possible, preferably at least once an hour.

To download updates, Kaspersky Anti-Virus connects to the Kaspersky Lab's update servers accessible via the Internet: an http or an ftp updates server specified by the user or to a local or a network folder accessible to your computer. The selection of the resource to be used depends on the settings (details see section 7.1.1 on page 63).

Updates can be downloaded automatically according to the schedule (see section 7.5 on page 101) or manually (see section 6.1.2 on page 47). To download updates, your computer must be connected to the Internet.

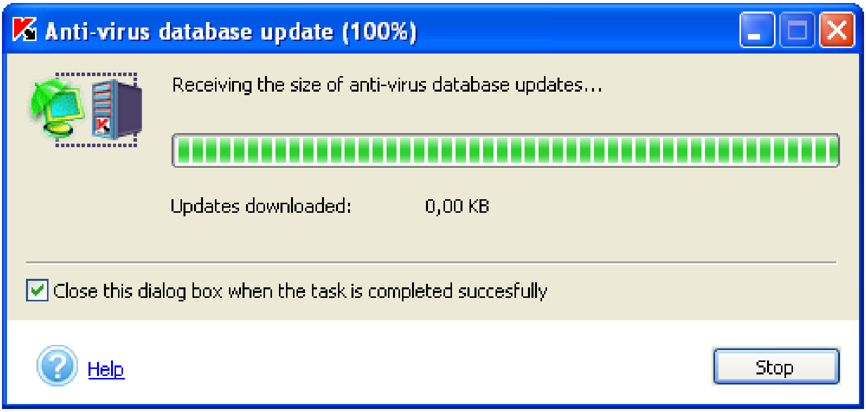
The process of downloading updates can be divided into the following stages:

1. Kaspersky Anti-Virus checks the network connection and establishes the connection with the updates source.
2. The application receives the list of the size of the updates.
3. The application compares the status of the anti-virus database and of the application modules of Kaspersky Anti-Virus installed on your computer with those provided by the source. If you have the latest version of the anti-virus database installed on your computer, the update procedure will then be completed. Otherwise the application will

start copying files to your computer. The downloading process is displayed by a progress bar (see Figure 9).

4. The application connects the downloaded database. If the database is connected successfully, Kaspersky Anti-Virus will start using this database when performing a scan. If connection to the database resulted in an error, the application will automatically roll back to the database version used earlier.

After the updates have been received and connected, you may need to restart your computer. In this case a corresponding pop-up message will be displayed.



Anti-virus database update (100%)

Receiving the size of anti-virus database updates...

Updates downloaded: 0,00 KB

☑ Close this dialog box when the task is completed succesfully

Figure 9. The **Anti-virus database update** dialog box

6.1.1. When should you download updates?

The application will notify you when your anti-virus database needs updating. You can also check the status of your anti-virus database in the right section of the **Protection** tab (see Figure 5), which will offer advice.

The following symbols are used to reflect the status of the anti-virus database:

✓ your anti-virus database has been recently updated or is being updated at the moment.

⚠ *your anti-virus database must be updated*. If updating is impossible because your license has expired, the application offers you information about renewing your license.

✖ an urgent update is required as the current anti-virus database is extremely outdated, missing or corrupted.

6.1.2. On-demand updates

In order to download the anti-virus database updates:

select the **Update Anti-Virus Database** item in the shortcut menu that opens by pressing the Kaspersky Anti-Virus icon in the system tray.

or

use the Update now link in the left part of the **Protection** tab (see Figure 5).

or:

use the Update the anti-virus database link in the right part of the **Protection** tab (see Figure 5). This link is displayed if the anti-virus database has not been updated for a long time.

On-demand or scheduled downloading can only be initiated if your computer is connected to the Internet. If an Internet connection is unavailable, the updating process will not start.

6.2. Real-time protection

Real-time protection of your computer is provided only if you did not disable it during the installation of the application.

Real-time protection of your computer means that Kaspersky Anti-Virus Pro constantly monitors all potentially unsafe actions performed on your computer as far as anti-virus and network security are concerned. The list of such actions include opening a file, saving a modified file, viewing incoming mail and sending outgoing mail, running scripts in Microsoft Internet Explorer as well as actions performed by potentially dangerous scripts, such as VBScript, JavaScript and macrocommands that are used by office applications.

When any of these actions are attempted, Kaspersky Anti-Virus scans the corresponding object, and then, depending on the scan results, either permits or prohibits the action. If a malicious object is detected, a notification will be displayed on the screen.

Thus, when operating in the real-time protection mode, the application performs several independent functions:

- real-time file protection (see section 7.2.1 on page 71);
- real-time mail monitoring (see section 7.2.2 on page 76);
- VBA macros monitoring (see section 7.2.3 on page 82);
- real-time scripts monitoring (see section 7.2.4 on page 83)
- real time protection against network attacks (see section 7.2.5 on page 85).

Each of the functions can be configured independently or even be disabled as this does not affect the performance of other real-time protection components.

6.2.1. Checking the protection status

The current real-time protection status is displayed in the right-hand section of the **Protection** tab (see Figure 5) in the main application window.

The real-time protection status is indicated by the following icons:

✓	*real-time protection is enabled* and the protection settings match the recommended settings.
⚠	*real-time protection is enabled*, but the protection settings do not match the recommended settings.
⏸	*anti-virus protection is stopped*. This status indicates that the protection of your computer has been temporarily disabled.
✖	*real-time protection is not working*. In this case we recommend to configure the real-time protection parameters (see section 7.2 on page 71) and then enable it.

6.2.2. Stopping real-time protection

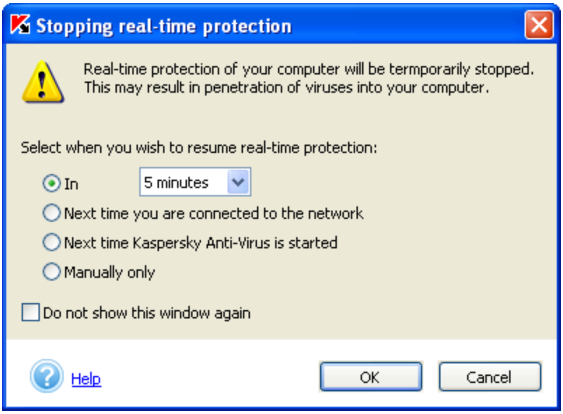
Sometimes during your work you may need to stop real-time protection. In order to do this, open the Kaspersky Anti-Virus shortcut menu and select the **Stop Real-Time Protection** (see section 5.2 on page 36).

As disabling anti-virus protection completely is not recommended, Kaspersky Anti-Virus will suggest that you stop it.

Select one of the following options in the **Stopping real-time protection** window (see Figure 10):

- **In 5/10/15 minutes** – the protection will be enabled after the specified period of time.
- **Next time you are connected to the network** – the protection will be enabled immediately after your computer connects to the network (this option appears in the list if the computer is currently disconnected from the network).
- **Next time Kaspersky Anti-Virus is started** – protection will be enabled if you start the program from the **Start** → **Programs** → **Kaspersky Anti-Virus Personal Pro** menu or after the system restart (provided that the automatic program start a the system startup mode is enabled).
- **Manually only** – In order to enable real-time protection select **Resume Real-Time Protection** from the Kaspersky Anti-Virus shortcut menu.

If necessary, you can also completely disable one of the application components: file system protection (see section 7.2.1 on page 71), mail protection (see section 7.2.2 on page 76), macros monitoring (see section 7.2.3 on page 82), scripts monitoring (see section 7.2.4 on page 83) or protection against network attacks (see section 7.2.5 on page 85).



Stopping real-time protection

Real-time protection of your computer will be termporarily stopped.
This may result in penetration of viruses into your computer.

Select when you wish to resume real-time protection:

● In 5 minutes
○ Next time you are connected to the network
○ Next time Kaspersky Anti-Virus is started
○ Manually only

□ Do not show this window again

Figure 10. Temporarily disabling anti-virus protection

6.3. On-demand scan

On-demand computer scan is a mode of operation of Kaspersky Anti-Virus used for scanning user's computer for malicious code and initiated either by the user's request or according to the schedule.

Kaspersky Anti-Virus Personal Pro allows to perform a full or a partial scan of the user's computer; the partial scan may involve individual drives, folders, files or mail. During the scan the application disinfects or deletes the detected dangerous objects and quarantines suspicious objects.

The following on-demand scan tasks are created during the installation of Kaspersky Anti-Virus by default:

- **Scan My Computer** – a full scan of the entire file system of the user's computers (see section 6.3.2 on page 51), by default this type of scan starts every Friday at 8.00 pm.
- **Scan removable drives** – a scan of removable media drives (diskette, CD, flash card, etc.); this type of scan is by default manually initiated by the user (see section 6.3.5 on page 57).
- **Scan critical areas** - by default the scan of system memory, automatic startup objects, and system folders Windows and Windows/system32 is manually initiated.
- **Scan Quarantine** - scanning of quarantined objects; by default is initiated manually by the user.
- **Scan at Kaspersky Anti-Virus startup** – a scan of the startup objects, system memory and boot sectors; by default this type of scan is started automatically at the operating system startup.

Additionally, the application provides for scanning objects specified by the user (details see section 6.3.3 on page 52). Besides you can create additional on-demand scan tasks by yourself (see section 7.3.1 on page 89).

6.3.1. When do I need to perform an anti-virus scan?

Even if, as a result of an on-demand scan of selected objects, no viruses are found, this does not guarantee that your computer is virus-free. Therefore, Kaspersky Anti-Virus always checks whether your entire computer has been scanned for viruses.

During a full scan, the application scans more objects stored in your computer than it does in the real-time protection mode. Therefore, we recommend that you scan your computer at least once a week, as a preventive measure.

The application will remind you when it is the best time to start a full scan. In case the main application window is closed, a pop-up window containing a recommendation to start a full scan will appear above the Kaspersky Anti-Virus icon in the system tray (if pop-ups are not disabled, see section 8.6 on page 120).

For more detailed information, open the main application window and see the full scan status in the right section of the **Protection** tab (see Figure 5). The full scan status is represented by one of the following icons:

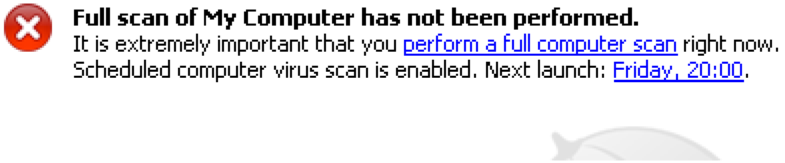
✓ A full scan is performed on a regular basis or is being performed at the moment;

⚠ *You should perform a full computer scan now*. You may also need to restore the recommended settings before you start the scan;

✗ It is extremely important that you perform a full computer scan now.

If required, you can also start a full scan directly from this tab by following the perform a full computer scan link.

Kaspersky Lab recommends that you schedule a full scan to start automatically. The full scan status indicates whether the scheduled scan mode is enabled.



Full scan of My Computer has not been performed.
It is extremely important that you perform a full computer scan right now.
Scheduled computer virus scan is enabled. Next launch: Friday, 20:00.

Figure 11. Information about the necessity of a full scan

6.3.2. Starting an on-demand scan

To start an on-demand anti-virus scan of your entire computer:

click Scan My Computer in the left section of the **Protection** tab (see Figure 5)

or

select item **Scan My Computer** in the shortcut menu that opens when you press the Kaspersky Anti-Virus icon in the system tray.

After this a **Scan** dialog box (see Figure 8) will open. This dialog box displays the percentage of the scan progress, the name of the object currently scanned, the estimated time of the scan completion and the general statistical data about the number of objects scanned and objects that have been disinfected, deleted and quarantined.

⚠ The full computer scan does not include the analysis of mailboxes (see section 6.3.3 on page 52), and removal drives (see section 6.3.5 on page 57) and network drives if such drives are connected to your computer.

You can hide the scan window (see Figure 8) by pressing the ☒ button in the right top corner and select the ● **Close this dialog box and resume scan** option.

You can view the scan results in a report (for more details refer to section 8.4 on page 114).

6.3.3. On-demand scan of selected objects

Sometimes you need to scan particular objects rather than the entire computer. Such objects may include, for example, a hard drive with program files and games, email databases that you have brought from the office, an archive attached to an email message that you have received. You can select objects to be scanned by using either Kaspersky Anti-Virus or standard Microsoft Windows tools (for example, **Windows Explorer**, **My Computer**, etc.).

To scan an object selected using standard Microsoft Windows tools:

select and right-click the object you wish to scan and when the Microsoft Windows shortcut menu appears, select the **Scan for viruses** command (see Figure 12).

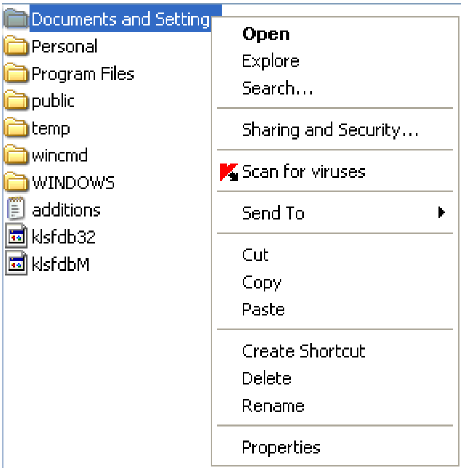


Figure 12. Scanning an object using standard Microsoft Windows tools

To select and scan objects using Kaspersky Anti-Virus Pro follow the following steps:

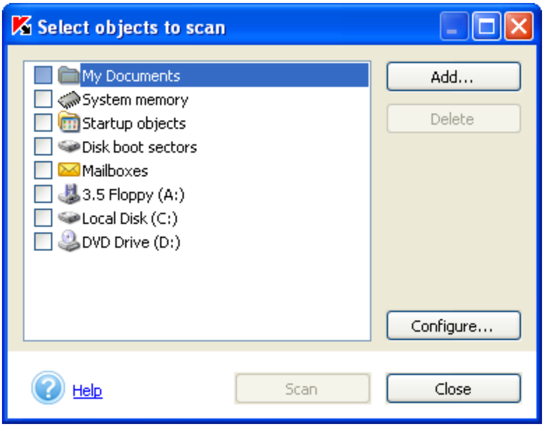
To select and scan an object using Kaspersky Anti-Virus Personal Pro:

click Scan objects in the left section of the **Protection** tab (see Figure 5).

The **Select objects to scan** window opens (see Figure 13), containing a list of objects that can be scanned for viruses, and equipped with interface buttons for editing this list and controlling the scan.

The initial list includes the following objects:

- removable drives, including floppy disks and CD-ROM;
- hard drives;
- Microsoft Office Outlook and Microsoft Outlook Express mailboxes;
- **My Documents** folder.
- System memory;
- Startup objects;
- Disk boot sectors;



□ My Documents
□ System memory
□ Startup objects
□ Disk boot sectors
□ Mailboxes
□ 3.5 Floppy (A:)
□ Local Disk (C:)
□ DVD Drive (D:)

Figure 13. Selecting objects to be scanned

To add a new object to the list, click **Add** and in the file selection window, browse to the file or folder you wish to add. All added objects will be available in this list for future scans.

When you create the path to a folder to an object you can use the system environment variables. For example, you can select the Microsoft Windows operating system installation folder to be scanned by specifying **%windir%** as the variable.

To delete an object from the list, check the corresponding box ☑ and click **Delete**. Note, however, that you can delete from the list only those objects that you have added manually. Objects that were included in the initial list cannot be deleted.

If you wish to alter the selected object(s) scan settings, use the **Configure** button. The settings you have entered will be saved for later scanning of the objects included in the list created and for scanning objects selected using standard Microsoft Windows tools.

To select and scan objects from the list:

1. Select objects you wish to scan from the list.
2. Click **Scan** to start the scan.

Regardless of how the scan was started (from Kaspersky Anti-Virus or from the Microsoft Windows shortcut menu), the **Scan** window will appear (see Figure 8). The scan results are documented in a report (see section 8.4 on page 114).

If any objects require regular scan, you can create a corresponding on-demand scan task (details see section 7.3.1 on page 89).

6.3.4. Scanning archives

Kaspersky Anti-Virus scans archives if the **Maximum Protection** or **Recommended** protection level is selected and if these archives have not been previously excluded from the scope of the scan (see section 7.2.2.1 on page 78).

Kaspersky Anti-Virus Personal Pro scans all objects contained within archives, but disinfects only *zip, arj, cab, rar, lha and ice* archives.

Kaspersky Anti-Virus DOES NOT disinfect self-extracting archives!

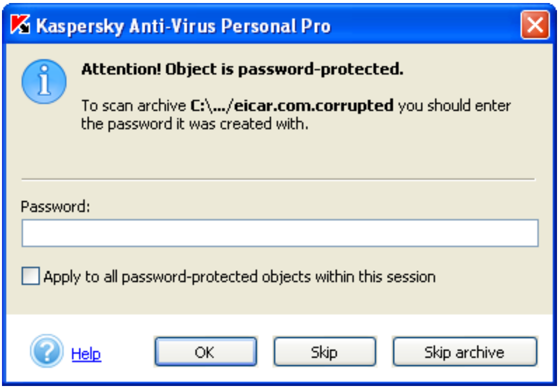
If an archive or an object within an archive is protected with a password and the mode of prompting for the password is enabled, you will be prompted for the password before scanning continues (see Figure 14). If you selected the mode of delayed objects processing (that is if you selected the **Prompt user for action once the scan is completed** action in the scan settings, see section 7.3.2.2 on page 95), the prompt for the password will be displayed once the scan is complete.

You can enable or disable the prompt for password by checking the ☑ **Do not ask for password when scanning objects** box in the on-demand scan settings window (see section 7.3.2.1 on page 92). By default the box is unchecked only for the **Maximum protection** level.

In the **Password** field, enter the password required to access this archive or an object within this archive and click **OK**. The archive, and all objects contained within it, will be scanned after the password is entered.

While processing objects within archives, Kaspersky Anti-Virus unpacks an archive to a temporary folder, scans the objects, processes them, packs them into a new archive with the same name and copies this new archive to the initial location of the original archive, thus overwriting the existing original archive. A similar procedure is used for processing password-protected objects within archives. Note that after the objects have been processed, they will be packed into a new archive with no password.

If another password-protected archive is found within the archive being scanned, Kaspersky Anti-Virus tries to apply the password used to access the first (containing) archive to the second (contained) archive. You will only be asked to enter a new password if the password is invalid.



Kaspersky Anti-Virus Personal Pro

Attention! Object is password-protected.

To scan archive **C:\.../eicar.com.corrupted** you should enter the password it was created with.

Password:

□ Apply to all password-protected objects within this session

Figure 14. Entering password to scan an archive

If you do not want to scan a particular password-protected object within an archive, click the **Skip** button and proceed with the scan.

If you do not know the password, the application will be unable to scan this password-protected archive and the objects contained within it. We recommend that you click **Skip archive** and proceed with the scan.

When you check the ☑ **Apply to all password-protected objects within this session** box, the action that you select after checking this box will be applied to all password-protected objects.

For example, if you check this box and click **Skip archive** button, all password-protected archives will be skipped during this scan.

If you enter the password, check the box and click the **OK** button, then this password will be automatically used to access all password-protected objects within all archives in this session. If the password is invalid for a certain object, that object will be skipped.

When an infected object is detected in an archive Kaspersky Anti-Virus will make an attempt to disinfect this object. If disinfection is not possible the object will be deleted from an archive.

If an archive cannot be disinfected and **Perform recommended action** is selected in the on-demand scan settings as an action to perform upon the detection of dangerous object, Kaspersky Anti-Virus will not delete an archive and will only write the information about its detection to report.

If the actions **Prompt user for action once the scan is completed** or **Prompt user for action** are selected in the on-demand scan settings (see section 7.3.2.2 on page 95), you will be able to delete the archive that cannot be disinfected by choosing **Delete** action in the window of inquiry of actions upon the detection of a dangerous object (see Figure 15). Besides you can delete the given archive manually.

6.3.5. Scanning removable drives

Your computer can easily be infected with viruses residing on floppy disks, CDs, and other removable media. If a floppy disk (or a bootable CD) you have used was infected with a boot virus, and you rebooted with the disk left in your drive, this may have gravest consequences to your system.

We recommend that you scan all removable media before using them.

You can scan removable media either from the Kaspersky Anti-Virus main window or by using the Microsoft Windows shortcut menu accessed from **Windows Explorer**, **Desktop**, etc.

To scan removable media for viruses from the Microsoft Windows shortcut menu:

select and right-click the drives (you can select the CD-ROM and the floppy disk at the same time). When the Microsoft Windows shortcut menu appears, select **Scan for viruses** (see Figure 12).

To scan a CD-ROM or a floppy disk for viruses from the main application window of Kaspersky Anti-Virus:

1. Insert the disk into the CD-ROM drive or the floppy disk into the floppy drive. Note that the application can scan both the CD and floppy disk at the same time.

2. Click Scan removable drives in the left section of the **Protection** tab (see Figure 5). This hyperlink is displayed if the **Display task on the "Protection" tab** box (see Figure 34) in the information section of the task is checked.

or

Using the Scan objects link, go to the **Select objects to scan** window (see Figure 13), select removable drives and press the **Scan** button.

or

Select the **Settings** tab in the main application window and follow the On-Demand Scan tasks link. This will open the **On-Demand Scan tasks** window (see Figure 35). Select the **Scan removable drives** task in the list and press the **Run** button.

You can view the scan progress (percentage competed) in the **Scan** window that opens immediately after the scan is started (see Figure 8).

If you select only one removable drive for scanning, Kaspersky Anti-Virus will prompt you to insert the disk into the next removable drive after the scan is completed.

Note the following application features:

- If the CD or floppy disk drive is empty or disconnected, the drive will not be scanned. No message will be displayed.
- A CD, floppy disk or other removable medium inserted into its drive after the scan has started will not be scanned.
- If you eject the CD or floppy disk, or disconnect the drive while the scan is in progress, the application will enter error information into the report but no message will be displayed. After this the next removable drive, if one exists on your computer, will be scanned.

Each time a new removable drive is connected to the system (i.e. when the drive is detected by the system as new hardware), Kaspersky Anti-Virus will scan for boot-viruses provided that the real-time file protection is enabled.

6.4. Dealing with viruses

The actions performed by Kaspersky Anti-Virus upon detection of the dangerous object, malicious program or object, possibly infected with a virus or virus modification, depend on the real-time protection and on-demand scan settings that you have specified. This chapter discusses situations in which Kaspersky Anti-Virus offers a choice of actions to be performed on dangerous objects during the scan or when the scan is complete.

Such situations occur when you select the following actions to be performed on objects:

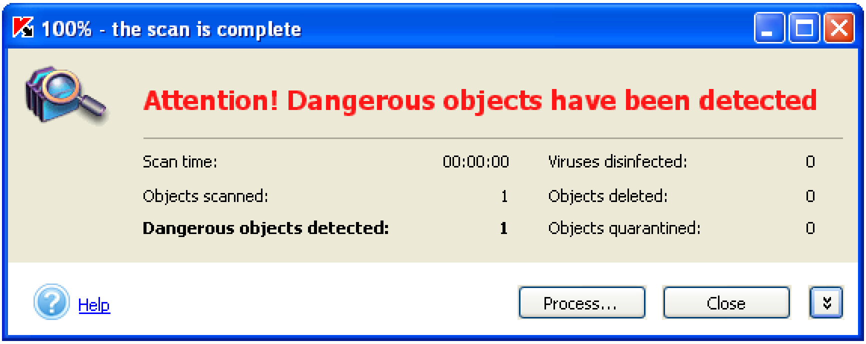
- Real-time protection (see section 7.2.1.2 on page 75):

  ◉ **Prompt user for action**. In this case the user will be prompted for action immediately when a dangerous object is detected.

- On-demand scan (see section 7.3.2.2 on page 95):

  ◉ **Prompt user for action during the scan**. The application will offer you to select an action to be performed with a dangerous object when it is detected by Kaspersky Anti-Virus or

● **Prompt user for action once the scan is completed**. The application offers to select an action to be performed with dangerous objects only if you have initialized processing of these objects - pressed the **Process…** button in the scan results window (see Figure 15).



100% - the scan is complete

Attention! Dangerous objects have been detected

Scan time:	00:00:00	Viruses disinfected:	0
Objects scanned:	1	Objects deleted:	0
Dangerous objects detected:	**1**	Objects quarantined:	0

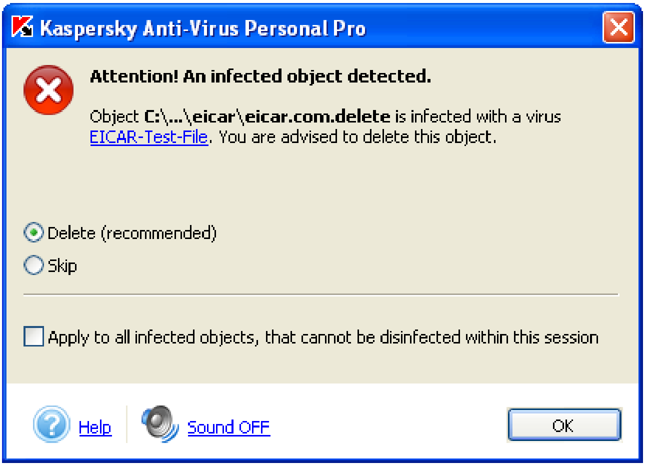
Figure 15. Delayed processing of dangerous objects

Upon detection of a dangerous object a message will be displayed (see Figure 16), containing:

- a detailed description of the object with an indication of the name of the dangerous program;
- a list of possible actions that you can perform on this object. This list always contains an action recommended by Kaspersky Lab, which is flagged by the word "recommended". Depending on the type of detected object, you may be offered the following actions:
  - **Disinfect** – attempt to disinfect the infected object, if disinfection is possible. When object is disinfected for the first time it's copy will be saved in the backup storage.
  - **Delete** – delete the infected or possibly infected object. A copy of the object to be deleted will be saved in the backup storage.
  - **Skip** – do not perform any actions; write information on this object into the report.

⚠ A dangerous object will be skipped if you close the window with the notification about its detection by clicking the ☒ button in the top right corner.

- **Quarantine** – quarantine the suspicious object so that later it can be checked, restored, sent to Kaspersky Lab for analysis or deleted.
- **Skip, add to exclusions** – add the detected object to the list of exclusions from anti-virus scan and protection.



Kaspersky Anti-Virus Personal Pro

Attention! An infected object detected.

Object **C:\...\eicar\eicar.com.delete** is infected with a virus EICAR-Test-File. You are advised to delete this object.

● Delete (recommended)

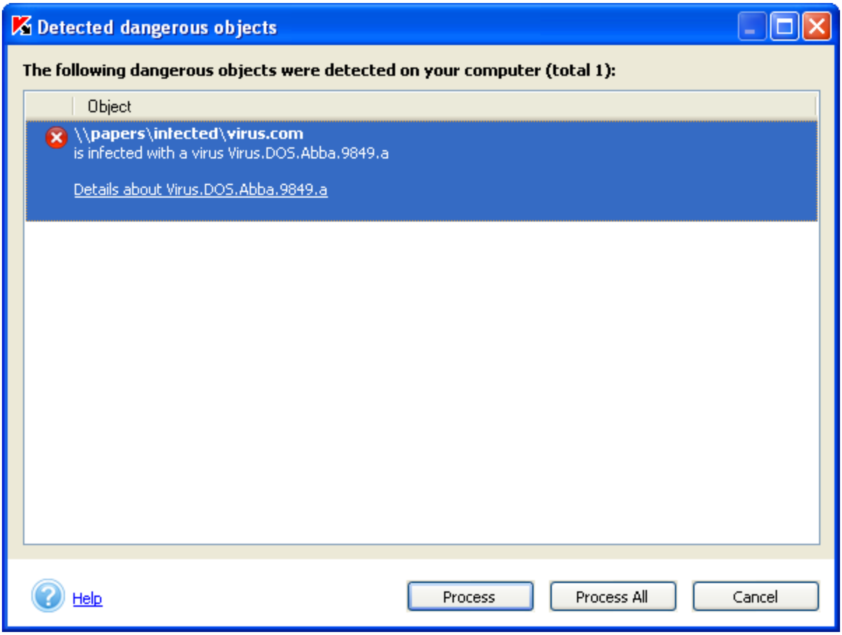
○ Skip

□ Apply to all infected objects, that cannot be disinfected within this session

Figure 16. A message about the detection of an infected object

You can also apply the selected action to all objects of the same type by checking the corresponding checkbox. Thus, to apply the selected action to all infected objects that can be disinfected, check the ☑ **Apply to all infected objects, that cannot be disinfected within this session** box.

If, for any reasons, you decided not to process objects by selecting the **Skip** option, you can still perform this processing at a later time. In order to do this, follow the process these objects link in the right section of the **Protection** tab. This will open the **Detected dangerous objects** dialog box (see Figure 17), that contains a detailed description of each of the dangerous object detected and the link to the description of the selected object at www.viruslist.com.



Detected dangerous objects

The following dangerous objects were detected on your computer (total 1):

Object
\\papers\infected\virus.com is infected with a virus Virus.DOS.Abba.9849.a Details about Virus.DOS.Abba.9849.a

Figure 17. The list of detected dangerous objects

By pressing the **Process** button, you can process the object selected in the list or you can start processing all objects in the list by pressing **Process All**. As the result, the application will display messages (see Figure 16) where you can select an action to be performed with the object (detailed description of possible actions see above).

In order to delete an object from the list without processing, use the **Remove from the list** command from the shortcut menu (see Figure 18).

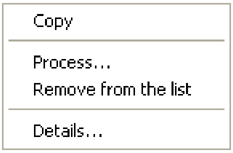


Figure 18. Shortcut menu of the **Dangerous objects detected** dialog box

If any of dangerous objects was deleted manually, it will be removed from the list of detected dangerous objects when another processing attempt is performed.

CHAPTER 7. CONFIGURING THE APPLICATION

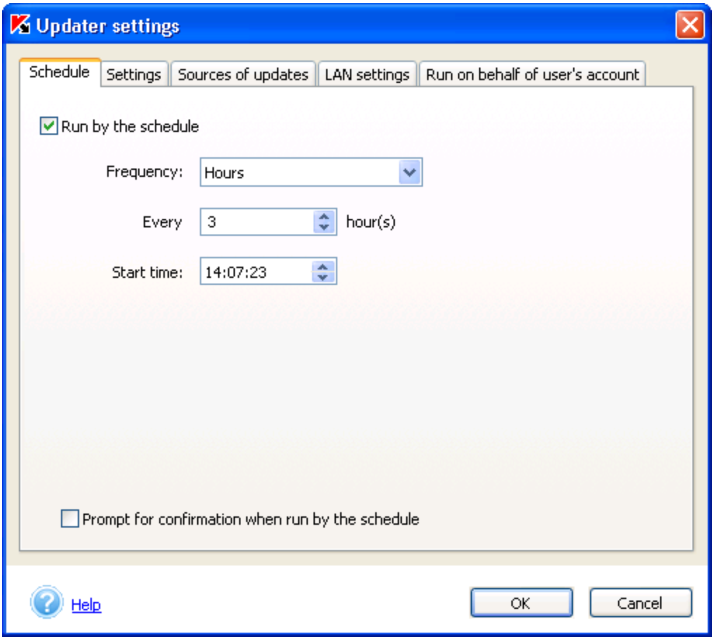
7.1. Configuring updates

In order to configure the anti-virus database updating settings,

follow the Configure Updater link located in the left section of the **Settings** tab.

This will open the updating settings configuration dialog box (where, using various tabs, you can configure the following functions:

- set up an automatic update starting schedule (see section 7.6 on page 103).



Updater settings

☑ Run by the schedule

Frequency: Hours

Every 3 hour(s)

Start time: 14:07:23

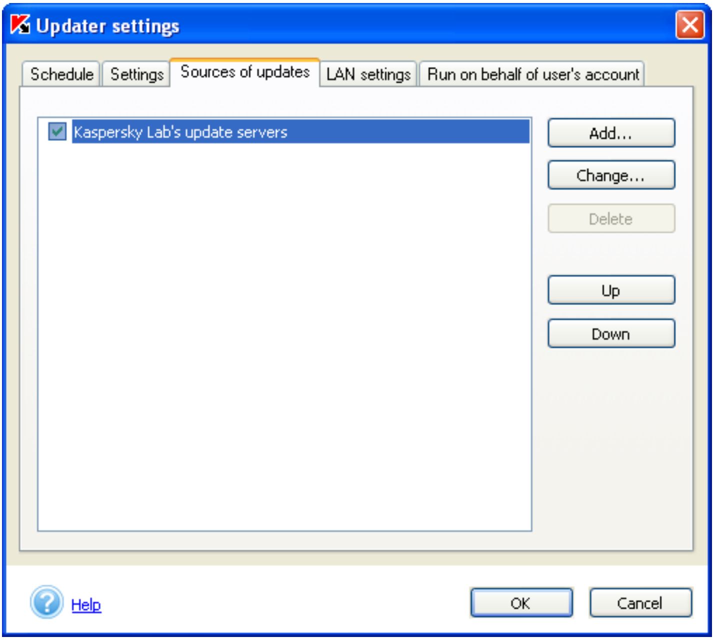
□ Prompt for confirmation when run by the schedule

Figure 19. Configuring the anti-virus database updating task settings
Schedule tab

- enable Kaspersky Anti-Virus application modules updating functions (see section 7.1.3 on page 67)
- select the updates source: Kaspersky Lab's servers, an http or an ftp server specified by her user or a local or network folder accessible to the user's computer (see section 7.1.1 on page 63)
- set up proxy server settings (see section 7.1.2 on page 65)
- set up tasks to be run under another user's account (only for computers running Microsoft Windows NT/2K/XP) (see section 7.7 on page 106).
- select the type of anti-virus database to be downloaded (see section 7.1.4 on page 68).

7.1.1. Selecting the updates source

You can select the updates source on the **Sources of updates** tab of the **Updater settings** dialog box (see Figure 20).



☑ Kaspersky Lab's update servers

Figure 20. **Updater settings** dialog box.
Sources of updates tab

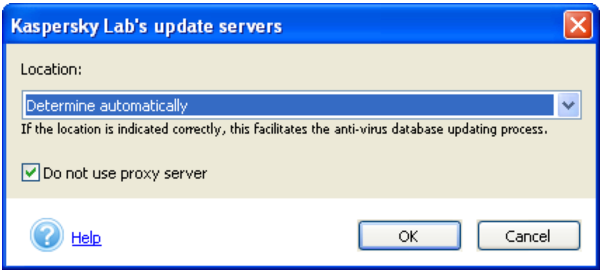
You can specify the source, from which the updates will be performed, as follows:

- *Kaspersky Lab's updates servers* - Kaspersky Lab's internet sites to which updates anti-virus database and application modules are uploaded.
- *ftp, http servers*, added by the user and containing new updates.
- *a local or a network folder.*

By default the updates are performed from the internet using the Kaspersky Lab's updates servers. You can expand the list by adding additional updates servers. In order to do this, press the **Add** button and select the source type - a *server* or a *folder*. If you choose the server option, enter the address of the ftp or the http server in the window that will open (when you specify the server name, include the protocol prefix that you intend to use, for example: *http://server.net* or *ftp://10.0.0.1).* If you select the *folder* option, specify the path to the folder that contains the updates.

You can alter the updates source settings by pressing the **Change…** button. You can change the *URL* if you have selected an update server as the source or you can change the *path* if your selected source is a folder.

After you pressed the **Change…** button you can indicate the region of the Kaspersky Lab's server from which the updates must be copied. To do this, select the corresponding country from the **Location** drop-down list (see Figure 21). By default the country is determined based on the regional settings of your operating system. In order to determine the server closest to you geographically, we recommend you to specify your current location. This will help reduce time and increase speed of downloading the updates. Using this window you can also disable the use of proxy server by checking the corresponding box.



Kaspersky Lab's update servers

Location:

Determine automatically

If the location is indicated correctly, this facilitates the anti-virus database updating process.

☑ Do not use proxy server

Figure 21. **Updater settings** dialog box.
The **Kaspersky Lab's update servers** tab

In order to ensure that the update is performed from the source you specified, check the ☑ box next to the name of this source. You can select several resources at the same time. If, by any reason, a selected source is unavailable, the update will be performed from the source next in the list, etc. You can alter the order of the update sources in the list by using the **Up** and **Down** buttons.

If you do not have access to the Kaspersky Lab's updates server (for example, if you do not have internet access), you can call our main office at +7 (495) 797-87-00 and find out the address of a closest Kaspersky Lab's partner that can provide the anti-virus database on a diskette or a disk in zip format.

When ordering anti-virus database, remember to specify what type of database you would like to receive: standard or extended or redundant (see s.7.1.4 on page 69)

Upon the receipt, unzip the zip archive with the anti-virus database into any folder on your computer and specify this folder as the updates source.

7.1.2. Configuring proxy server parameters

If you use a proxy server to connect to the internet, contact your internet service provider or your system administrator to find out whether you have to specify the proxy server parameters, namely the IP address or name, port and the authorization settings.

By default, for updating the anti-virus database Microsoft Internet Explorer internet connection settings will be used. If you use a proxy server for the internet connection, contact your internet service provide or your system administrator to find out whether you have to specify the proxy server parameters, namely IP address or name, port, authentication parameters, etc.

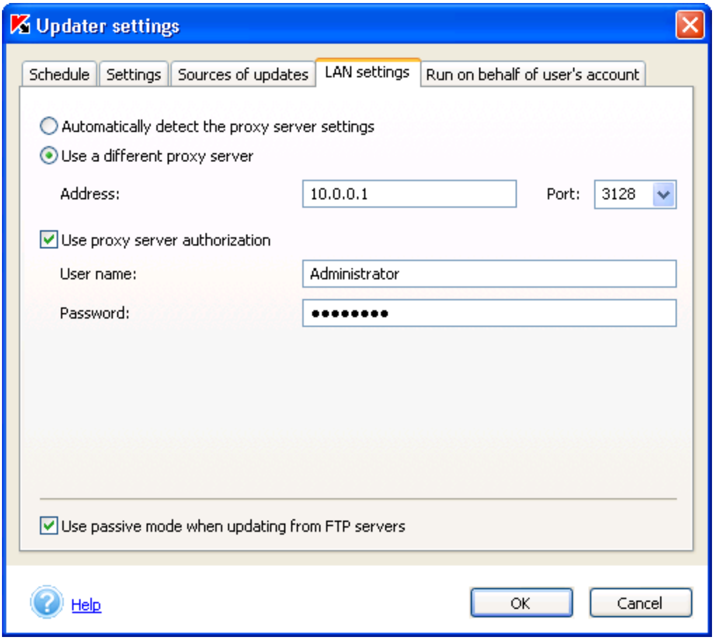
The network connection parameters are configured in the **LAN settings** tab (see Figure 22). There are two ways to define the parameters of the proxy server:

- ● **Automatically detect the proxy server settings**
- ● **Use a different proxy server**

The first option is selected by default; the proxy server parameters will be copied from Microsoft Internet Explorer. If your proxy server requires authorization, select the second option and specify the proxy server settings manually.

Address – IP-address of the proxy server in the format aaa.bbb.ccc.ddd or its name.

Port – port number where the proxy server is located. Select one of the values from the dropdown list: 3128, 8080, 8082, 8903 or enter a different value.



○ Automatically detect the proxy server settings

● Use a different proxy server

Address: 10.0.0.1 Port: 3128

☑ Use proxy server authorization

User name: Administrator

Password: ●●●●●●●●●

☑ Use passive mode when updating from FTP servers

Figure 22. Configuring the proxy server settings

If your proxy server requires authorization, check the ☑ **Use proxy server authorization** checkbox and specify your username and password in the text fields below as required.

If proxy server authorization is required and you have not specified name and password or if the name and the password entered have not been accepted by the proxy server for some reason, the application will prompt you for the username and the password when the updating process is initiated. If the authorization was successful, the application will use these username and password next time the update is performed. Otherwise you will be asked to re-enter the authorization parameters.

To determine the geographically closest to you Kaspersky Lab update server, select your current location from the **Location** drop-down list. This will help to reduce the time and to increase the speed of updates download.

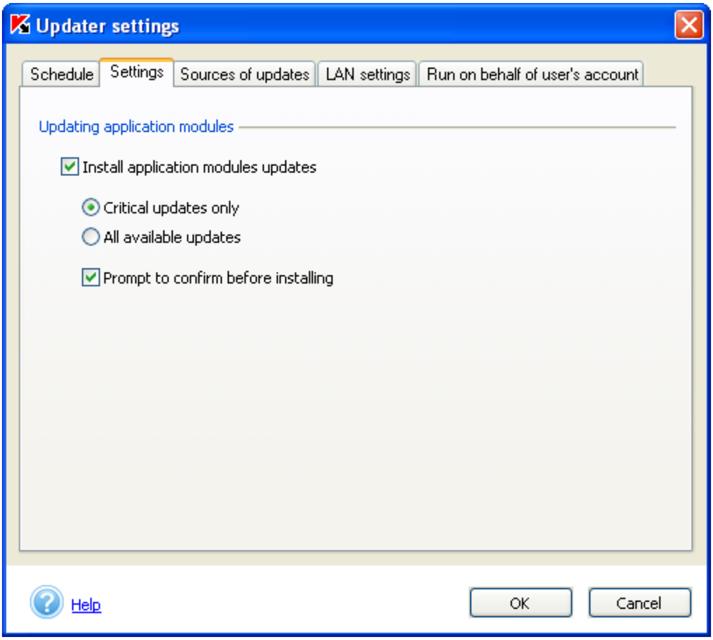
If you have a firewall installed on your server and you cannot connect to the FTP site in the active mode, check the ☑ **Use passive mode when updating from FTP servers** box.

7.1.3. Updating Kaspersky Anti-Virus application modules

In addition to the anti-virus database, you can also update Kaspersky Anti-Virus application modules. Application module updates are uploaded to the Kaspersky Lab's update servers from time to time, as such modules are released.

You can update application modules from the source specified during updates source configuration (see section 7.1.1 on page 63). To do this, check the ☑ **Install application modules updates** box in the **Settings** tab of **Updater settings** dialog box (see Figure 23) and select which updates you would like to install:

- **Critical updates only**
- **All available updates**



Updating application modules

☑ Install application modules updates

● Critical updates only

○ All available updates

☑ Prompt to confirm before installing

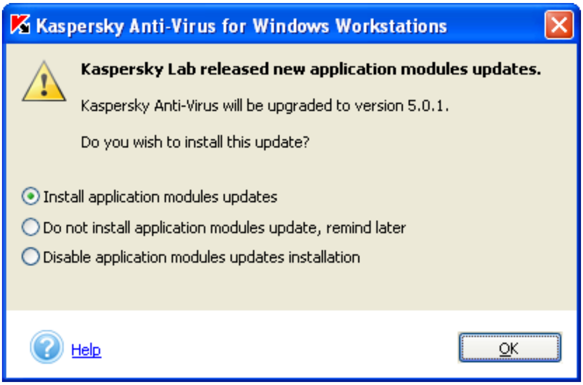
Figure 23. The **Updater settings** window.
The **Settings** tab

If you wish the modules to be automatically installed after they are downloaded, uncheck the ☑ **Prompt to confirm before installing** box. By default after the updates are downloaded a prompt to confirm their installation is displayed on the screen.

If you order a zip archive with the updates from Kaspersky Lab or from our partners, make sure you mention that you would like to receive the application modules updates as well.

When you receive the application modules update a corresponding prompt will be displayed on the screen (see Figure 24). Select one of the following options.

- **Install application modules updates**
- **Do not install application modules updates, remind later** – remind about the installation of the application modules updates next time you run Kaspersky Anti-Virus.
- **Disable application modules updates installation** – if you select this option, the ☑ **Install application modules updates** in the **Settings** tab of the **Updater settings** box (see Figure 23) will be unchecked and the application modules updates installation will be disabled.



Kaspersky Anti-Virus for Windows Workstations

Kaspersky Lab released new application modules updates.

Kaspersky Anti-Virus will be upgraded to version 5.0.1.

Do you wish to install this update?

● Install application modules updates

○ Do not install application modules update, remind later

○ Disable application modules updates installation

Figure 24. Prompt for installation of the application modules

7.1.4. Which anti-virus database should be used

Kaspersky Anti-Virus offers to use any of the two types of anti-virus database with the application:

- *Standard anti-virus database* - the anti-virus database that contains records about all malware known at the moment and about methods used for treating this malware.
- If you wish to protect data stored on your computer against potentially dangerous programs, you have to use *Extended anti-virus database*. In addition to records contained in the standard database, this database contains description of adware, spyware hacking tools and other riskware.

Redundant database, as well as extended database, allows detecting riskware, but in addition, it contains more records that include description of remote surveillance, adware, automatic dialing programs that connect the user's computer to commercial internet sites and programs that are not riskware but may constitute a part of software for development of malicious programs.

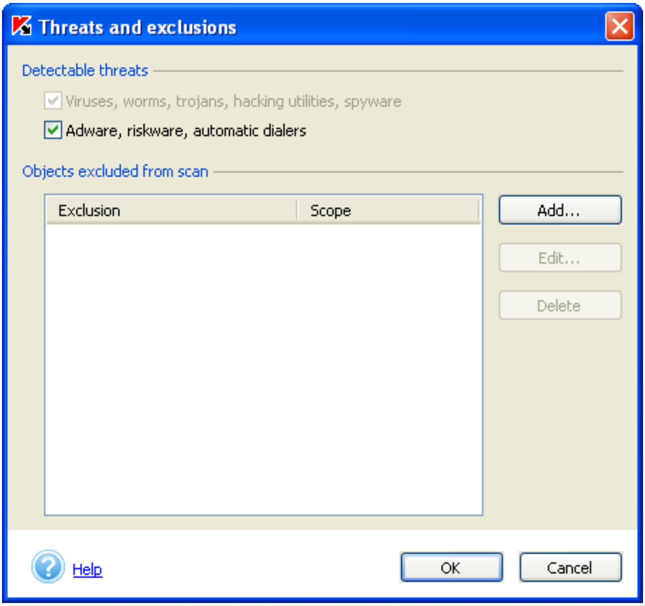
The use of standard anti-virus database is sufficient to ensure regular anti-virus protection of your computer. The use of the extended anti-virus database may affect the speed of your Kaspersky Anti-Virus operation. Besides, some programs that you use may be treated as riskware.

In order to select the anti-virus database type to be used with your Kaspersky Anti-Virus Personal Pro,

1. Follow the Threats and exclusions link in the left section of the **Settings** tab (see Figure 6).

2. In the dialog box that will open (see Figure 25), check the ☑ **Adware, riskware,and automatic dialers** box in the **Detectable threats** section if you wish to use the extended anti-virus database. If you would like to prevent the removal of applications that you use, we recommend that you select an action to be performed with a dangerous object that requires confirmation by the user (see section 7.3.2.2 on page 95).

Box ☑ **Viruses, worms, trojans, hacking utilities, spyware** is checked by default and cannot be unchecked. It shows that the standard anti-virus database is used for scanning.



Threats and exclusions

Detectable threats

☑ Viruses, worms, trojans, hacking utilities, spyware

☑ Adware, riskware, automatic dialers

Objects excluded from scan

Exclusion	Scope

Figure 25. Selecting the type of the anti-virus database.

7.2. Configuring real-time protection

In order to configure the real-time protection settings on your computer use the Configure Real-Time Protection link located in the left part of the **Settings** tab (see Figure 6).

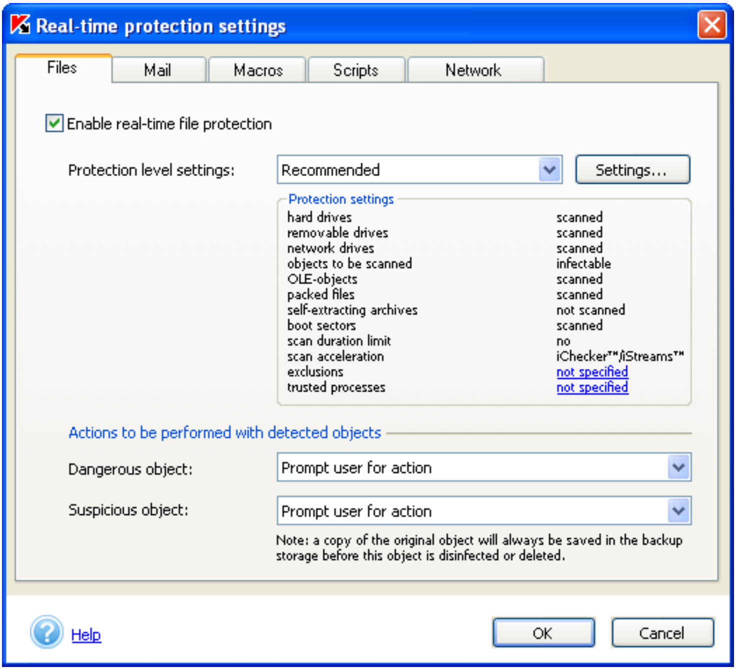
The real-time protection dialog box contains several tabs to represent various protection functions. Each function is discussed in detail below.

7.2.1. File protection

If file protection is installed and enabled in the real-time protection mode, Kaspersky Anti-Virus will analyze all calls to the computer's file system for the presence of malicious code.

In order to configure the real-time file protection you must switch to the **Files** tab of the **Real-time protection settings** dialog box (see Figure 26) where you can:

- enable/disable protection by checking or unchecking the ☑ **Enable real-time file protection** box. By default this box is checked and protection is enabled;



☑ Enable real-time file protection

Protection level settings: Recommended

Protection settings

hard drives	scanned
removable drives	scanned
network drives	scanned
objects to be scanned	infectable
OLE-objects	scanned
packed files	scanned
self-extracting archives	not scanned
boot sectors	scanned
scan duration limit	no
scan acceleration	iChecker™/iStreams™
exclusions	not specified
trusted processes	not specified

Actions to be performed with detected objects

Dangerous object: Prompt user for action

Suspicious object: Prompt user for action

Note: a copy of the original object will always be saved in the backup storage before this object is disinfected or deleted.

Figure 26. Configuring real-time file protection

- select one of the anti-virus protection levels and also configure settings of the level selected (see section 7.2.1.1 on page 73);
- create a list of objects that will not be scanned in the real-time file protection mode (see section 7.4 on page 97). In order to switch to the dialog box where you can create a list of exclusions, follow the specified / not specified link next to the **exclusions** section in the description of the protection settings selected. The text of the link toggles depending on whether the exclusions have been configured.
- create a list of trusted processes the file activity of which will not be scanned by the real-time file protection feature (see section 7.5 on page 101).
- specify the action that will be performed by Kaspersky Anti-Virus when a dangerous or a suspicious object is detected (see section 7.2.1.2 on page 75).

If the real-time file protection feature is not installed, settings listed above cannot be configured. In order to install the file protection feature, you will have to re-install the application.

7.2.1.1. Selecting the protection level

Select one of the levels pre-defined by the Kaspersky Lab's experts in from the **Protection level settings** drop-down list (details see Chapter 4 on page 30). By default the recommended level anti-virus protection setting will apply.

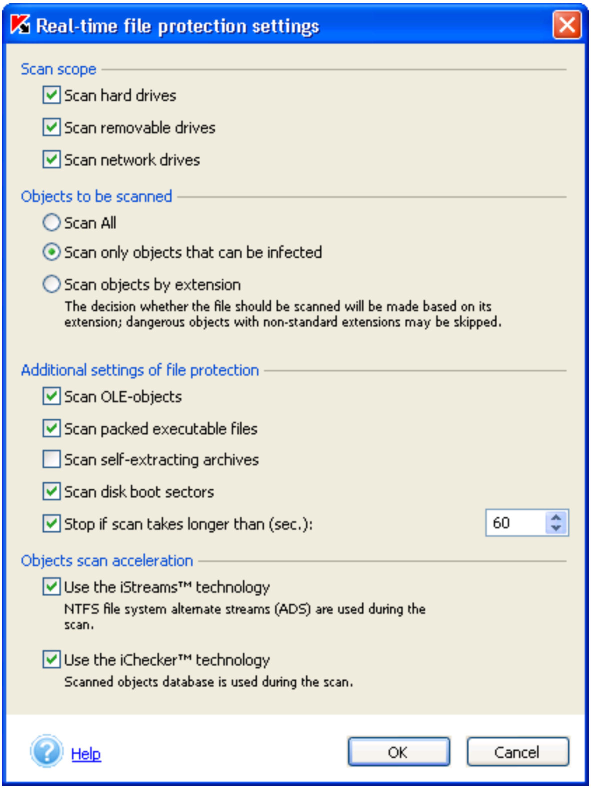
Based on the settings of any protection level you can configure your own settings. This protection level will change to the **User-defined settings**. When you return to the settings of any of the pre-defined levels the user-defined settings will not be saved.

You can view and alter the settings of the chosen protection level in the **Real-time file protection settings** window (see Figure 27) that opens by pressing the **Settings...** button in the **Files** tab (see Figure 26).

Check boxes to select drives to be scanned in the **Scan scope** section.

Select objects to be included into the scan scope in the **Objects to be scanned** section as follows:

- **Scan All** - scan files irrespective of their types and extensions;
- **Scan only objects that can be infected** - scan only those files that can potentially be infected; the analysis is based on the internal structure of the file;
- **Scan objects by extension** - scan files that can potentially be infected; the analysis is based on the file extension.



Real-time file protection settings

Scan scope

☑ Scan hard drives

☑ Scan removable drives

☑ Scan network drives

Objects to be scanned

○ Scan All

● Scan only objects that can be infected

○ Scan objects by extension

The decision whether the file should be scanned will be made based on its extension; dangerous objects with non-standard extensions may be skipped.

Additional settings of file protection

☑ Scan OLE-objects

☑ Scan packed executable files

□ Scan self-extracting archives

☑ Scan disk boot sectors

☑ Stop if scan takes longer than (sec.): 60

Objects scan acceleration

☑ Use the iStreams™ technology

NTFS file system alternate streams (ADS) are used during the scan.

☑ Use the iChecker™ technology

Scanned objects database is used during the scan.

Figure 27. Fine-tuning the real-time file protection settings

In the **Additional settings of file protection** section you can put a restriction on the single object processing time by specifying the scan interval in seconds and determine whether the scan includes:

- objects attached to or embedded into other files (OLE objects),
- packed executable files;
- self-extracting archives;
- disk boot sectors.

In the **Objects scan acceleration** section you can enable/disable the use of the anti-virus scan acceleration technologies - iChecker™ and iStreams™ (a detailed discussion of these technology see Appendix B on page 151). If you wish to use these technologies check the corresponding boxes.

If, during the installation of the application, you decided not to use the iStreams™ technology, then in order to enable it you will have to run the Kaspersky Anti-Virus installer again. Before you do it, you will not be able to use this technology.

7.2.1.2. Selecting an action to be performed with the object detected

In the **Actions to be performed with detected objects** (see Figure 26), specify the action that Kaspersky Anti-Virus will perform when it detects a dangerous or suspicious object.

- **Prompt user for action** - block access to the object and display a prompt for the user to select an action that should be performed with the object. This is the default mode.

  If the application does not receive your response within 30 seconds after the prompt is displayed, the recommended action will be applied to this object. Each type of objects has its own recommended action.

  Provided below is the list of all possible actions that are offered by Kaspersky Anti-Virus (the set of actions may differ for each type of objects):

  - *Disinfect* the infected object.
  - *Quarantine* the object that may be infected with a virus or its modification.

    Sometimes, as a result of putting a file into quarantine, a message may be displayed stating that the object cannot be deleted. This is related to the fact that when an object is moved to quarantine, it is copied to the quarantine and deleted from the original location. However, not any object can be deleted. For example, you cannot delete an object being in use by another application.

  - *Delete* a dangerous object that when disinfection has failed or cannot be performed.
  - *Skip* - do not perform any actions with the object, enter information about its detection into the report about the program's operation.

- **Perform the recommended action** - block access to the object, perform the action recommended for this object. The recommended action for infected objects is **Disinfect**, for possible infected object the recommended action is **Quarantine**, for trojans and worms - **Delete**.

- **Block access and delete** - block object and delete it without additional notification of the user about these actions. When the object is deleted, its copy is saved in the backup storage.
- **Block access only** - block access to the object, do not display any prompt for processing the object, enter information into the report.
- **Quarantine** (for suspicious objects only) - block access to the object, move the object to the quarantine folder for the subsequent processing using the updated anti-virus database, restoring, sending for analysis to Kaspersky Lab or deletion.

7.2.2. Mail protection

Real-time protection of the incoming and outgoing e-mail messages is ensured only if you decided to use this feature during the application installation. In order to install mail protection you will have to re-install the application.

Kaspersky Anti-Virus Personal Pro provides real-time protection for mail received by and sent from your computer.

Kaspersky Anti-Virus Personal Pro provides anti-virus protection of all mail received or sent by Microsoft Office Outlook (no matter which mail protocol is used) and mail received or sent by any e-mail client application using SMTP and POP3 protocols [5]. The mail is scanned at the moment it is received. Mail being sent is scanned irrespective whether you are sending it yourself or an attempt to send it is made by any application installed on your computer.

The scan for infected and dangerous objects is performed involving the body of the message and attached objects of any nesting level. When an infected object is detected in an e-mail message, by default a recommended action will be performed with this object: Kaspersky Anti-Virus Personal Pro will attempt to disinfect such object and if the disinfection is not possible - it will delete it from the e-mail message.

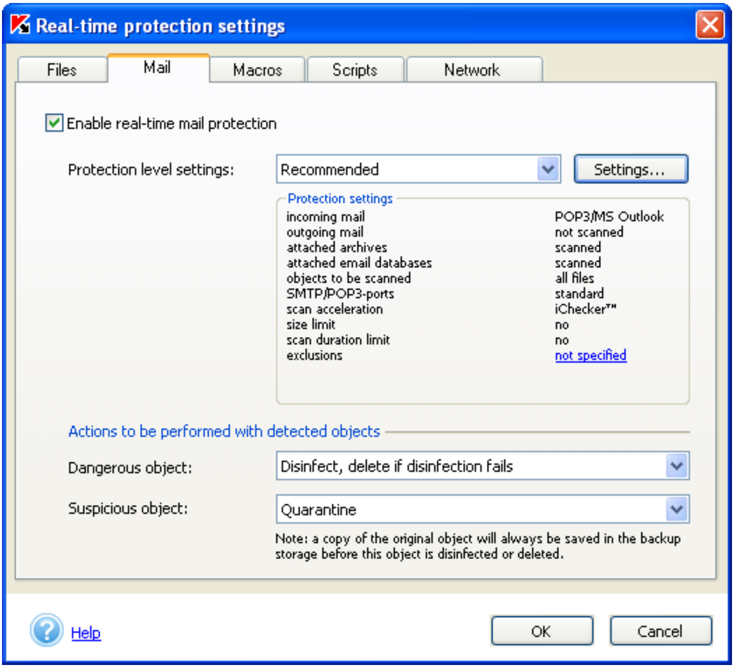
If you are working with e-mail messages stored on remote web servers using a browser, such as Microsoft Internet Explorer, the application will only scan files

[5] The application scans all mail received and sent by Microsoft Outlook irrespective of the mail protocols used as well as mail sent or received by any mail client application via STMP and POP3 mail protocols.

attached to the incoming e-mail messages at the moment these files are run or saved to the hard drive.

The real-time mail protection settings are configured in the **Mail** tab of the **Real-time protection settings** dialog box (see Figure 28). In this dialog box you can do the following:

- enable/disable protection by checking/unchecking the ☑ **Enable real-time mail protection** box. By default this box is checked and protection is enabled.
- select the anti-virus protection level and fine-tune the settings of the selected level (see section 7.2.2.1 on page 78).
- create a list of objects that will not be scanned in the real-time mail protection mode (see section 7.4 on page 97). In order to switch to the dialog box where you can create a list of exclusions, follow the specified / not specified link next to the **exclusions** settings in the description of the protection settings selected. The text of the link toggles depending on whether the exclusions have been configured;
- specify the action that will be performed by Kaspersky Anti-Virus when a dangerous or a suspicious object is detected (see section 7.2.2.2 on page 80).



☑ Enable real-time mail protection

Protection level settings: Recommended

Protection settings

incoming mail	POP3/MS Outlook
outgoing mail	not scanned
attached archives	scanned
attached email databases	scanned
objects to be scanned	all files
SMTP/POP3-ports	standard
scan acceleration	iChecker™
size limit	no
scan duration limit	no
exclusions	not specified

Actions to be performed with detected objects

Dangerous object: Disinfect, delete if disinfection fails

Suspicious object: Quarantine

Note: a copy of the original object will always be saved in the backup storage before this object is disinfected or deleted.

Figure 28. Configuring the real-time mail protection settings

7.2.2.1. Selecting the protection level

Select one of the levels pre-defined by the Kaspersky Lab's experts in from the **Protection level settings** drop-down list (details see Chapter 4 on page 30). By default the recommended level anti-virus protection setting will apply.

Based on the settings of any protection level you can configure your own settings. This protection level will change to the **User-defined settings**. When you return to the settings of any of the pre-defined levels the user-defined settings will not be saved.

You can view and alter the settings of the chosen protection level in the **Real-time mail protection settings** window (see Figure 29) that opens by pressing the **Settings...** button in the **Mail** tab (see Figure 28).

The upper part of the tab contains boxes that are used to specify types of objects to be scanned. If the box is checked, the application will intercept and scan objects of the corresponding type:

☑ **Scan mail received via POP3 protocol** – scanning incoming mail received using POP3 protocol for any mail client.

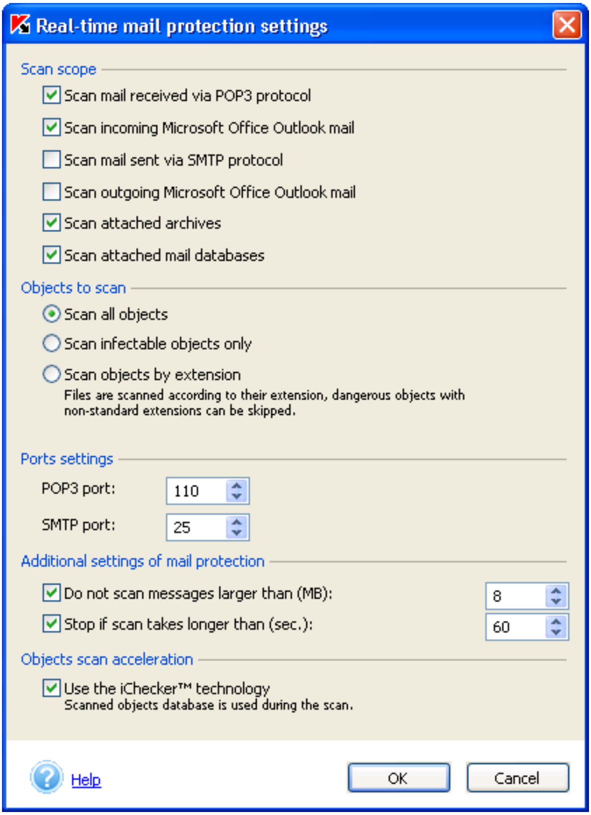
☑ **Scan incoming Microsoft Office Outlook mail** – scanning incoming mail when using Microsoft Office Outlook with any mail protocol.

☑ **Scan mail sent via SMTP protocol** – scanning outgoing mail being sent by STMP protocol by any mail client.

☑ **Scan outgoing Microsoft Office Outlook mail** – scanning outgoing mail when using Microsoft Office Outlook with any mail protocol.

☑ **Scan attached archives** – scanning archives attached to e-mail messages.

☑ **Scan attached mail databases**– scanning e-mail databases attached to e-mail messages.



Real-time mail protection settings

Scan scope

☑ Scan mail received via POP3 protocol

☑ Scan incoming Microsoft Office Outlook mail

☐ Scan mail sent via SMTP protocol

☐ Scan outgoing Microsoft Office Outlook mail

☑ Scan attached archives

☑ Scan attached mail databases

Objects to scan

● Scan all objects

○ Scan infectable objects only

○ Scan objects by extension
Files are scanned according to their extension, dangerous objects with non-standard extensions can be skipped.

Ports settings

POP3 port: 110

SMTP port: 25

Additional settings of mail protection

☑ Do not scan messages larger than (MB): 8

☑ Stop if scan takes longer than (sec.): 60

Objects scan acceleration

☑ Use the iChecker™ technology
Scanned objects database is used during the scan.

Figure 29. Fine-tuning the real-time mail protection settings

In the **Ports settings** section you can specify POP3 and SMTP mail port values that are used for data transfer. By default 110 and 25 ports will be used. If you mail client is using different ports, their numbers must be specified.

Additionally, you can put a restriction on the time and the size of the object being scanned:

☑ **Do not scan messages larger than (MB)**, in order to put a restriction on the size of the objects scanned, specify the maximum size of the objects to be scanned (in MB).

☑ **Stop if scan takes longer than (sec.)** - specify the scan time interval in seconds to put a restriction on the scan time.

In the **Object scan acceleration** section you can enable/disable the use of the anti-virus scan acceleration technology iChecker™ (a detailed discussion of the technology see Appendix B on page 151). If you wish to use this technology check the ☑ **Use the iChecker™ technology** box.

7.2.2.2. Selecting an action to be performed with an object detected

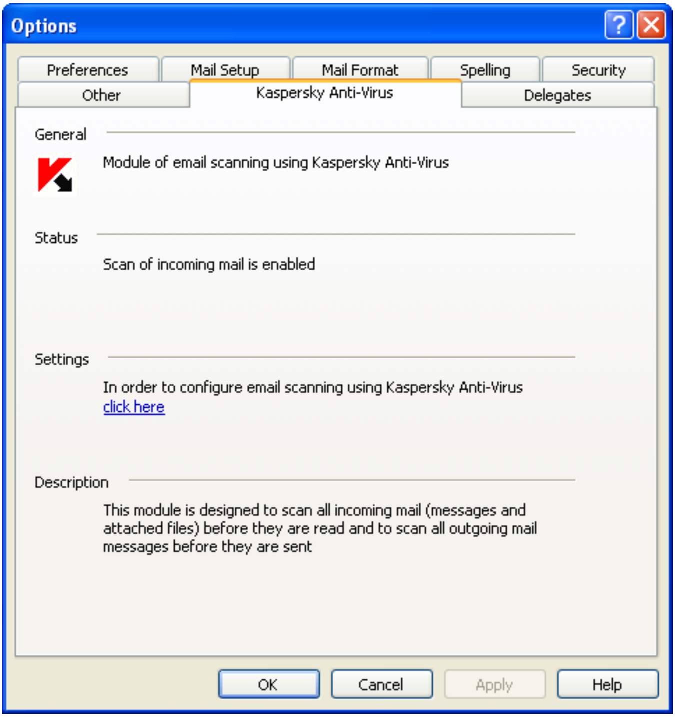
Specify the action that Kaspersky Anti-Virus will have to perform when a dangerous or suspicious object is detected in the **Actions to be performed with detected objects** section.

- **Disinfect, delete if disinfection fails** - attempt to disinfect a dangerous object, if the object cannot be disinfected - delete it.
- **Quarantine** - move a suspicious object into the quarantine folder for the subsequent rescan using updated anti-virus database, restoring, sending to Kaspersky Lab for analysis or deletion.
- **Delete** - delete dangerous or suspicious objects. If this action is selected, a copy of the object will created and placed into the backup storage. You can use this copy to restore the original object or forward it for analysis to Kaspersky Lab.

7.2.2.3. Scanning Microsoft Office Outlook mail

Microsoft Office Outlook mail is scanned using a dedicated module plugged-in into Microsoft Office Outlook. This module is used to scan all incoming mail (both messages and attached objects) before reading these messages and all outgoing messages - before sending them.

In order to open the mail scan window in the main Microsoft Office Outlook menu, select **Tools→Options**. In the **Options** window dialog box, switch to the **Kaspersky Anti-Virus** tab (see Figure 30).



General

Module of email scanning using Kaspersky Anti-Virus

Status

Scan of incoming mail is enabled

Settings

In order to configure email scanning using Kaspersky Anti-Virus click here

Description

This module is designed to scan all incoming mail (messages and attached files) before they are read and to scan all outgoing mail messages before they are sent

Figure 30. Kaspersky Anti-Virus tab in Microsoft Office Outlook

The **Status** section contains information about the mail scan module status. Depending on the actual status, the following messages are may be displayed.

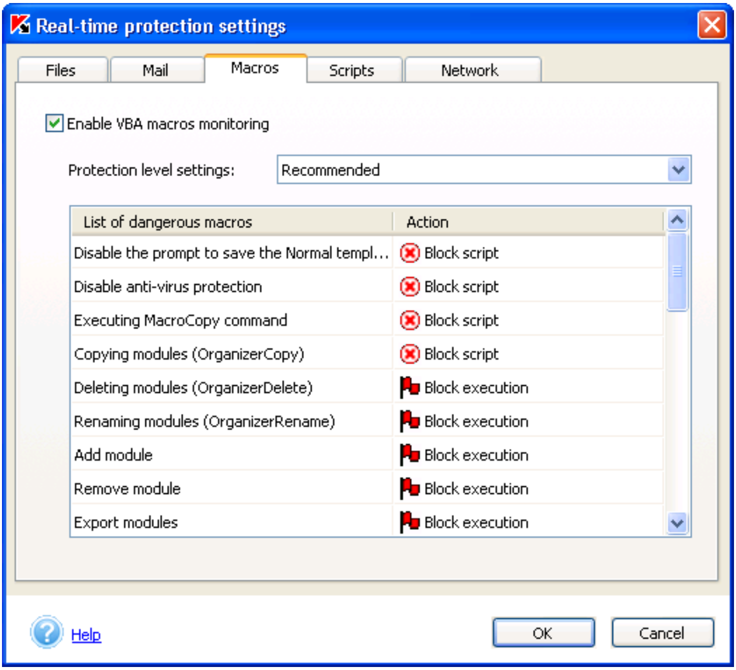
- *Scan of incoming and outgoing mail is enabled*. This message is displayed when Kaspersky Anti-Virus is started and the Microsoft Office Outlook mail protection function is enabled.
- *Scan of incoming mail is enabled*. This message is displayed if only incoming mail messages scan is enabled.
- *Scan of outgoing mail is enabled*. This message is displayed if only outgoing mail messages scan is enabled.
- *Email scan is disabled*. This message is displayed if the incoming and outgoing Microsoft Office Outlook mail is disabled or if Kaspersky Anti-Virus is closed.

To configure mail protection settings, use the click here link in the **Settings** section. This will open a real-time protection settings window on the **Mail** tab (see Figure 29).

7.2.3. Macros monitoring

If macros monitoring is installed and enabled in the real-time protection mode, Kaspersky Anti-Virus will analyze a set of VBA macros predefined by the application and prevents execution of any malicious code.

Macros monitoring settings are configured on the **Macros** tab of the **Real-time protection settings** dialog box (see Figure 31).



☑ Enable VBA macros monitoring

Protection level settings: Recommended

List of dangerous macros	Action
Disable the prompt to save the Normal templ...	Block script
Disable anti-virus protection	Block script
Executing MacroCopy command	Block script
Copying modules (OrganizerCopy)	Block script
Deleting modules (OrganizerDelete)	Block execution
Renaming modules (OrganizerRename)	Block execution
Add module	Block execution
Remove module	Block execution
Export modules	Block execution

Figure 31. Configuring real-time macros monitoring settings

By default macros monitoring is enabled. In order to disable this function, uncheck the ☑ **Enable VBA macros monitoring** box.

Select one of the levels pre-defined by Kaspersky Lab's experts in the **Protection level settings** drop-down list (see Chapter 4 on page 30).

The list of suspicious macros monitored by the application and the actions assigned for each macro according to the protection level selected are detailed in the table below:

- **Allow execution** – allow the execution of the macro, do not perform any actions.
- **Prompt for action** – prompt user for action by displaying a message.
- **Block execution** – block execution of the macro.
- **Block script** – stop execution of the script that called to the macro.

You can configure your own settings basing on the settings of any protection level. In this case the protection level will be changed to **User-defined settings**. After returning to the settings of one of the pre-defined protection levels, user-defined settings will not be saved.

In order to change the action to be performed by Kaspersky Anti-Virus when it detects a suspicious macro,

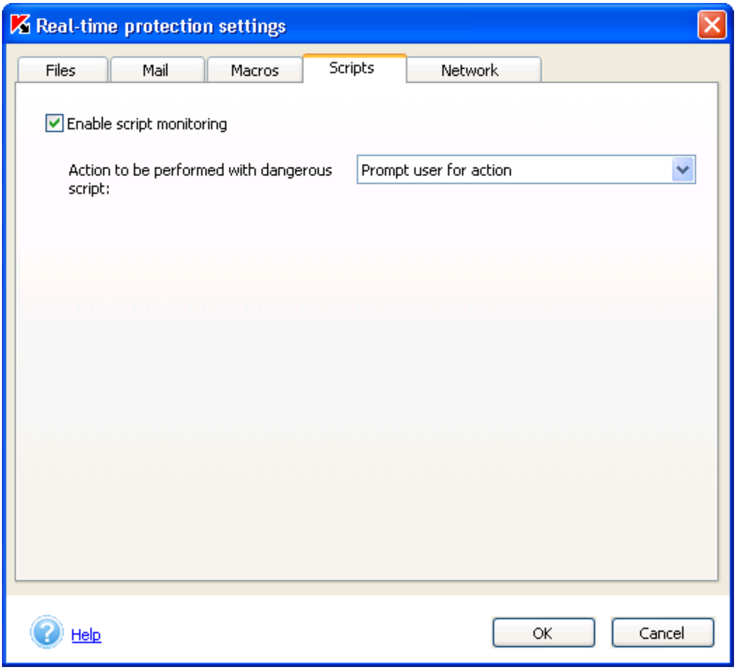
select a cell corresponding to the macro in the **Action** column in the table and select one of the above actions from the drop-down list.

7.2.4. Scripts monitoring

Protection of your computer against dangerous scripts is provided only if you did not disable it during the installation of the application.

If real-time monitoring is enabled in the real-time protection mode, Kaspersky Anti-Virus will analyze VBScripts and JavaScripts before their execution by the script processing module of the operating system and will prevent execution of any malicious code.

Script monitoring settings are configured in the **Scripts** tab of the **Real-time protection settings** dialog box (see Figure 32).



☑ Enable script monitoring

Action to be performed with dangerous script: Prompt user for action

Figure 32. Configuring real-time scripts monitoring settings

By default the script monitoring function is enabled. In order to disable it, uncheck the ☑ **Enable script monitoring** box.

Below this box, specify the action to be performed by Kaspersky Anti-Virus when it detects a dangerous script:

- **Prompt user for action** – display a warning about detection of a potentially dangerous script and prompt user for further actions. All possible actions will be listed in the prompt.
- **Block script execution** – block execution of scripts.
- **Allow script execution** – allow execution of scripts

When monitoring scripts in the Microsoft Internet Explorer status bar displays a blinking Kaspersky Anti-Virus icon .

7.2.5. Protection against network attacks

Protection of your computer against network attacks is provided only if you did not disable it during the installation of the application.

Kaspersky Anti-Virus Personal Pro 5.0 allows to protect your computer against network hacking attacks from the local area network or from the internet.

Hacking attacks are detected based on the records contained in the database of the attacks known at the moment. This database is updated and the updates are installed along with the update of the anti-virus database (details see Chapter 6 on page 45).

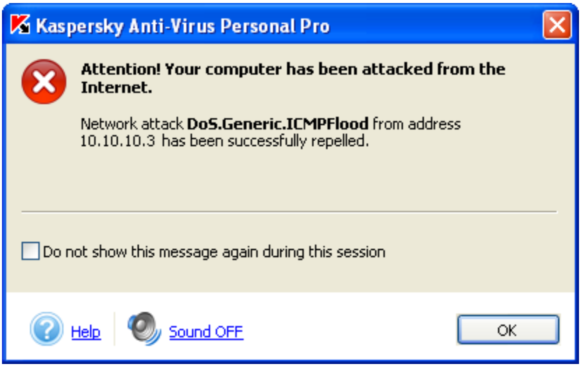
By default, protection against network attacks is started at Kaspersky Anti-Virus startup, monitors all network connections and checks all data received from the network irrespective of the source: local network or internet.

As an attempt to attack your computer occurs, this attack will be blocked. A corresponding notification will be displayed on the screen (see Figure 26) that will contain information about the type of attack, IP address of the attacking computer and the local port (if possible).

Settings of the real-time protection against network attacks are configured in the Network tab of the Real-time protection settings dialog box (see Figure 27).

When you enable or disable the real-time protection using the Kaspersky Anti-Virus context menu available via the system tray, the real-time protection against network attacks will also be disabled (see section 6.2.2 on page 48).

If you decide to disable only protection against network attacks while leaving other real-time protection functionality enabled, uncheck the ☑ **Enable real-time protection against network attacks** box (see Figure 34). In order to apply the changes you have made you will have to restart your computer.



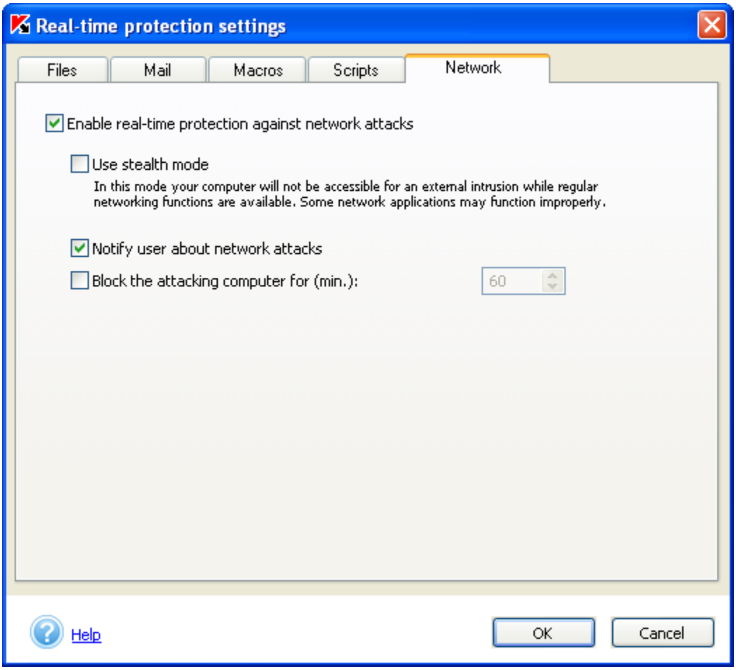
Kaspersky Anti-Virus Personal Pro

Attention! Your computer has been attacked from the Internet.

Network attack **DoS.Generic.ICMPFlood** from address 10.10.10.3 has been successfully repelled.

□ Do not show this message again during this session

Figure 33. Notification about a network attack



Real-time protection settings

☑ Enable real-time protection against network attacks

□ Use stealth mode

In this mode your computer will not be accessible for an external intrusion while regular networking functions are available. Some network applications may function improperly.

☑ Notify user about network attacks

□ Block the attacking computer for (min.): 60

Figure 34. Configuring real-time protection against network attacks

You can define Kaspersky Anti-Virus operation settings in the real-time network protection mode.

- **Stealth mode**. This mode allows only those network activities that have been initiated by the user or by programs installed on the user's computer; all other actions (remote connection to your computer, etc.) will not be allowed. This means that your computer becomes virtually "invisible" for other computers. Besides, the stealth mode allows to prevent any types of DoS (Denial of Service) attacks. At the same time, the stealth mode does not have any negative impact on your internet activities as Kaspersky Anti-Virus allows any network activities initiated by the user.

  Attention! Stealth mode does not protect your computer from the harmful actions of trojan programs!

  By default the stealth mode is disabled. In order to enable it, check the ☑ **Use stealth mode** checkbox.

- **Notifications about network attacks**. By default the program informs the user each time an attack is attempted at the computer. A message will be displayed (see Figure 33) containing information about the type of the attack, the IP address of the attacking computer and the local port (if it is possible to determine it). Since this notification is provided only for reference, you can disable its display by unchecking the ☑ **Notify user about network attacks** checkbox; the information about attacks will be entered into the reports.

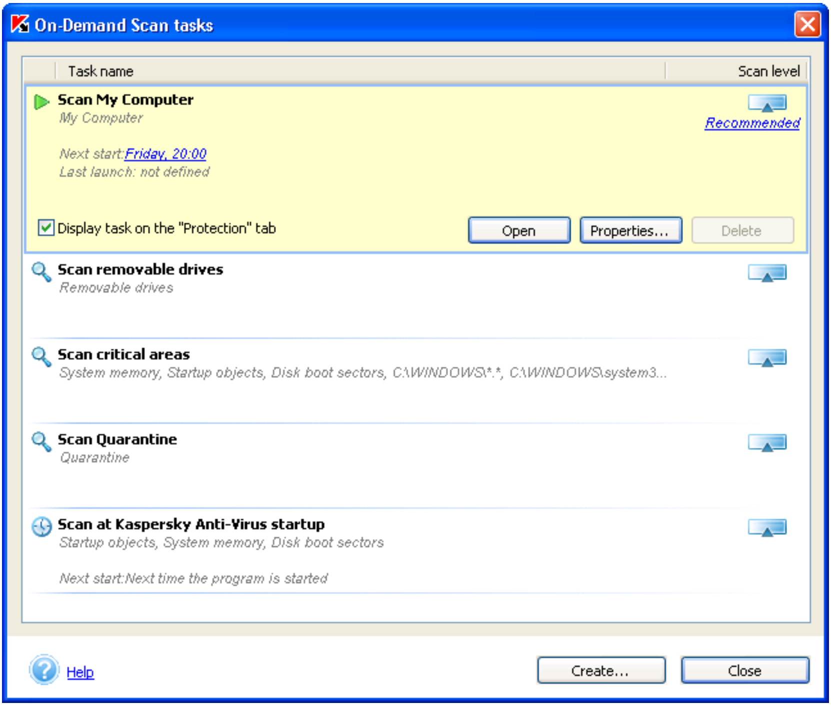
- **Blocking the attacking computer**. Kaspersky Anti-Virus Personal Pro can block all computers that attempt to attack your computer. By default the function of blocking the attacking computer is disabled. If you decide to enable this function, the default blocking time is 60 minutes. During this time, the any packets sent from the attacking computer to your computer will be blocked. In order to change the blocking period, specify the desired value in the ☑ **Block the attacking computer for (min.)** parameter. In order to disable the blocking mode, uncheck the checkbox beside this parameter.

7.3. Configuring on-demand scan settings

In order to view the list of all on-demand scan tasks,,

follow the On-Demand Scan tasks link located in the left part of the **Settings** tab (see Figure 6);

This will open the **On-Demand Scan tasks** dialog box (see Figure 35) that contains the list of all system tasks as well as additional tasks created by the user.



On-Demand Scan tasks

Task name	Scan level
▶ **Scan My Computer** *My Computer* *Next start: Friday, 20:00* *Last launch: not defined* ☑ Display task on the "Protection" tab	*Recommended*
Scan removable drives *Removable drives*	
Scan critical areas *System memory, Startup objects, Disk boot sectors, C:\WINDOWS*.*, C:\WINDOWS\system3...*	
Scan Quarantine *Quarantine*	
🕓 **Scan at Kaspersky Anti-Virus startup** *Startup objects, System memory, Disk boot sectors* *Next start: Next time the program is started*	

Figure 35. On-demand scan tasks list

Area that contains information about the scan area, time of last and next scan task run can be expanded by a click of a mouse. You can start a scan manually using the **Run** button in this area or open the scan task settings configuration dialog box using the **Properties…** button (see section 7.3.2 on page 90).

A brief explanation is provided for each task, including the scan scope next start date.

Depending on the situation the following icons may appear to the left of the task name:

🕓 – indicates that a schedule is set up for this task and it will be automatically started according to the schedule.

▶ – indicates that the task is being performed at the moment

If a scheduled task is in progress (see Figure 4) item **Started tasks** will appear in the context menu. If this item is selected, a submenu will open that contains a list of scheduled tasks currently running. In order to open the scan process window (see Figure 8), select a task from the list.

To the right of the tasks list are the control buttons using which you can: create new tasks, delete tasks from the list, run tasks, view or change settings and schedules for tasks or copy tasks. In order to execute any of the actions listed above, select a task from the list and press the corresponding button.

For viewing or editing the tasks settings, use the **Properties** button or double-click the name of the task in the list. In order to create an additional scan task, use the **Create** button. For more detailed information about creating and configuring tasks see section 7.3.1 on page 89 and section 7.3.2 on page 90.

In order to run a task, select it in the list and press the **Run** button. This will open a new window that contains information about execution of the task.

In order to create a new scan task based on the settings of an existing task, press the **Copy** button.

In order to create an additional scan task, use the **Create…** button in the **On-Demand Scan tasks** dialog box (see Figure 34). More details about creating a task see section 7.3.1 on page 89).

In order to delete a task, select it in the list and press the **Delete** button. However, bear in mind that you can delete only those tasks that were added manually, while the system tasks cannot be deleted. Also note that you cannot delete tasks that are currently being performed.

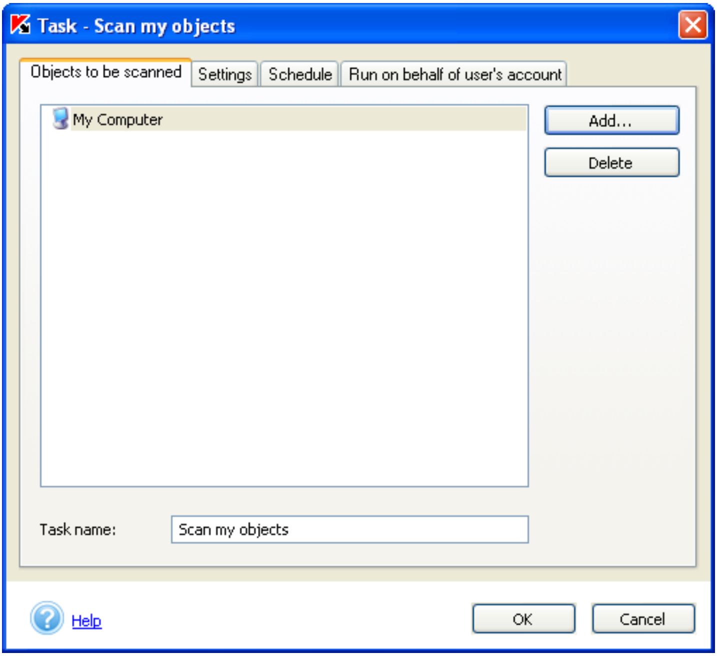
7.3.1. Creating a new task

In order to create a new on-demand scan task,

press the **Create** button in the **On-Demand Scan tasks** window (see Figure 35).

This will open an on-demand scan task properties dialog box (see Figure 36).

Enter the task name under which it will be displayed in the tasks list in the bottom part of the **Objects to be scanned** tab (see Figure 35). By default the task name is – **Scan my objects**. Then create a list of objects that will be scanned when this task is run in the **Objects to be scanned** section. In order to add a new object, press the **Add** button and select the object you need from the drop-down list. In order to scan an object not included into the list, for example an individual folder or a file, select the **Browse** line in the list and specify the path to this object. In order to delete the object from the list of objects to be scanned, select it in the list and press the **Delete** button.



Task name: Scan my objects

Figure 36. The **On-demand scan properties** dialog box

By default, the task will be executed using the recommended protection level settings (see Chapter 4 on page 30). If you wish, you can configure the on-demand scan settings (see section 7.3.2 on page 90).

If you plan to run a certain task often, we recommend that you check the ☑ **Display task in the "Protection" tab** box. In this case you will be able to run this task using a link with the same name located in the left part of the **Protection** tab (see Figure 5).

7.3.2. Configuring the scan settings

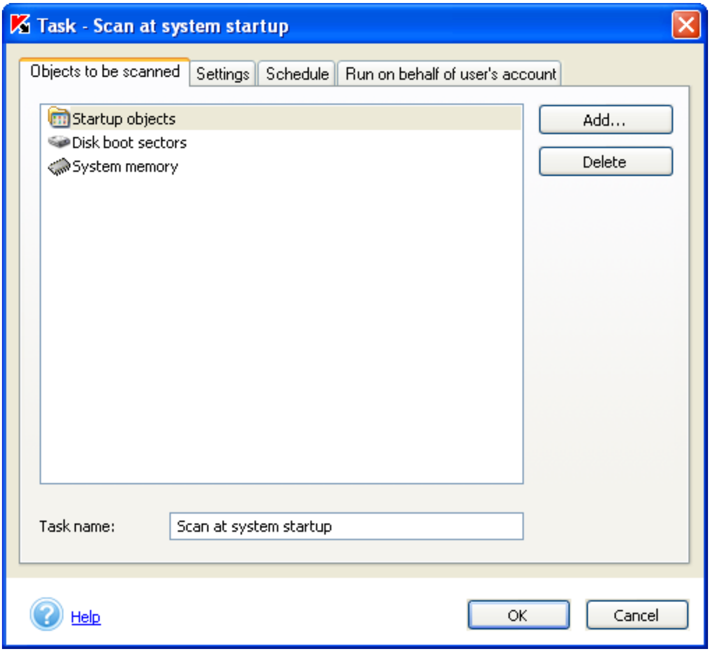
In order to configure the on-demand scan settings,

1. Use the On-Demand Scan tasks link located in the left part of the **Settings** tab (see Figure 6).

2. In the window that will open (see Figure 35) select the task you need from the list and press the **Properties** button.

This will open the scan settings dialog box (see Figure 37), where you can:

- select objects to be scanned. This feature is available for tasks that were created manually. In order to add a new object, press the **Add** button on the **Objects to be scanned** tab and select the required object from the drop-down list. In order to scan an object not included into the list, for example an individual folder or file, select the **Browse** line in the list and specify the path to such object. In order to exclude an object from the list of objects to be scanned, select it in the list and press the **Remove** button.



Startup objects
Disk boot sectors
System memory

Task name: Scan at system startup

Figure 37. Configuring the on-demand scan settings

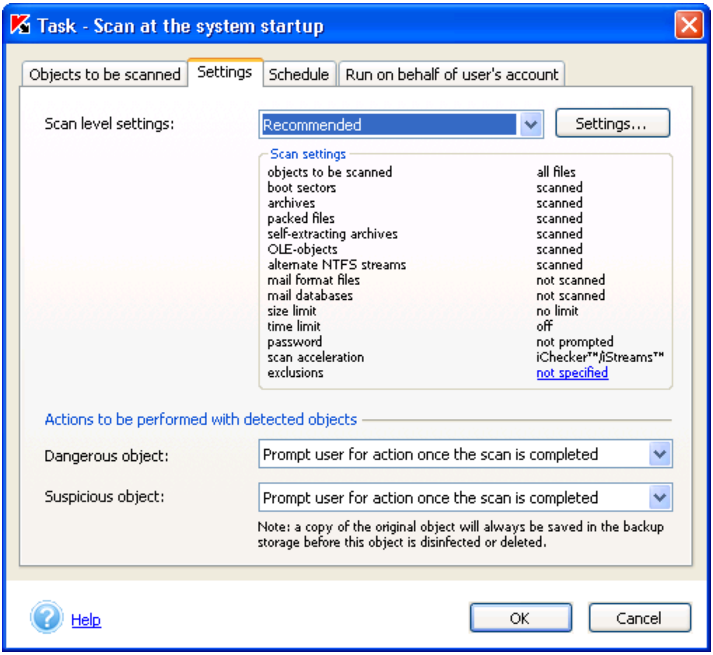
- specify the scan level and configure the scan settings (see section 7.3.2.1 on page 92);

- create a list of objects that will not be scanned (see section 7.4 on page 97). In order to switch to the dialog box where you can create a list of exclusions, follow the specified / not specified link next to the **exclusions** setting in the description of the protection settings selected. The appearance of the link toggles depending on whether the exclusions have been configured;

- specify actions that will be applied by Kaspersky Anti-Virus when a dangerous or a suspicious object is detected (see section 7.3.2.2 on page 95);
- set up a scan task start schedule (see section 7.5 on page 101) ;
- configure the task start on behalf of another user's account (only for computers running Microsoft Windows NT/2K/XP) (see section 7.7 on page 106).

7.3.2.1. Selecting the scan level

Select one of the three scan levels predefined by the Kaspersky Lab's experts from the **Scan level settings** drop-down list on the Settings tab (see Figure 38) (details see Chapter 4 on page 30). By default the recommended anti-virus protection settings will apply.


Task - Scan at the system startup
Objects to be scanned
Settings
Schedule
Run on behalf of user's account
Settings…
Help
OK
Cancel

Scan level settings: Recommended

Scan settings

objects to be scanned	all files
boot sectors	scanned
archives	scanned
packed files	scanned
self-extracting archives	scanned
OLE-objects	scanned
alternate NTFS streams	scanned
mail format files	not scanned
mail databases	not scanned
size limit	no limit
time limit	off
password	not prompted
scan acceleration	iChecker™/iStreams™
exclusions	not specified

Actions to be performed with detected objects

Dangerous object: Prompt user for action once the scan is completed

Suspicious object: Prompt user for action once the scan is completed

Note: a copy of the original object will always be saved in the backup storage before this object is disinfected or deleted.

Figure 38. Configuring on-demand scan

Based on the settings of any scan level you can configure your own settings. In this case scan level will change to **User-defined settings**. When you return to the settings of any of the pre-defined levels the user-defined settings will not be saved.

You can view and alter the settings of the chosen scan level in the **On-demand scan settings** window (see Figure 38) that opens by pressing the **Settings...** button (see Figure 37).

In the **Objects to be scanned** select object that will be scanned by the Kaspersky Anti-Virus:

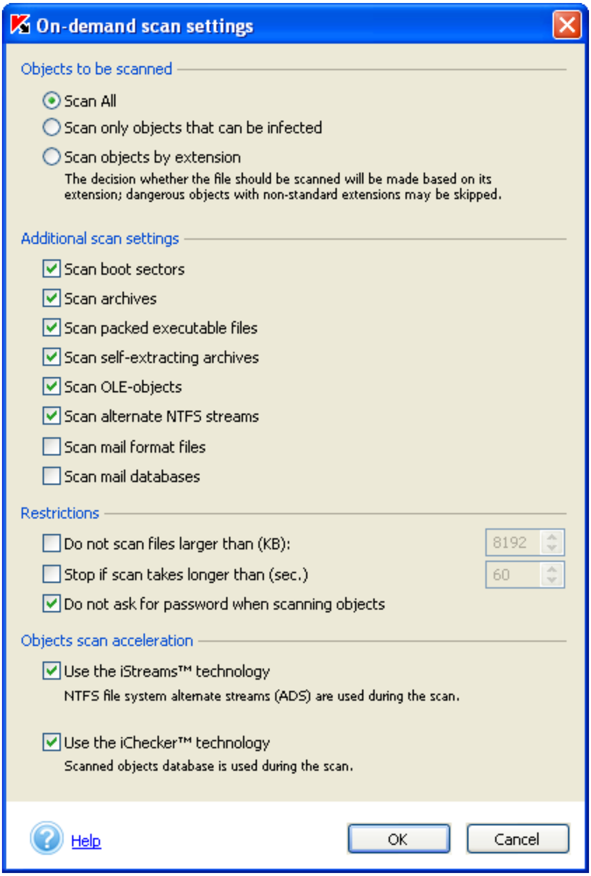
- **Scan All** – scan files irrespective of their type and extension.
- **Scan only objects that can be infected** – scan only those files that can potentially be infected; the analysis is based on the internal structure of the file;
- **Scan objects by extension** – scan files that can potentially be infected; the analysis is based on the file extension.

In the **Additional scan settings** you can specify whether you wish to scan:

- boot sectors’
- archives;
- packed executable files;
- self-extracting archives;
- objects attached to or embedded into other files (OLE objects),
- alternate NTFS streams;
- mail files;
- mail database;

Check the following boxes in the **Restrictions** sections as required:

- **Do not scan files larger than (KB)**, in order to put a restriction on the size of the objects scanned, specify the maximum size of the objects to be scanned (in KB).
- **Stop if scan takes longer than (sec.)** - specify the scan time interval in seconds to put a restriction on the scan time.
- **Do not ask for password when scanning objects**, so that when scanning password-protected objects the prompt for password is not displayed. If this box is checked, password-protected objects will be skipped during the anti-virus scan.



On-demand scan settings

Objects to be scanned

● Scan All
○ Scan only objects that can be infected
○ Scan objects by extension
The decision whether the file should be scanned will be made based on its extension; dangerous objects with non-standard extensions may be skipped.

Additional scan settings

☑ Scan boot sectors
☑ Scan archives
☑ Scan packed executable files
☑ Scan self-extracting archives
☑ Scan OLE-objects
☑ Scan alternate NTFS streams
□ Scan mail format files
□ Scan mail databases

Restrictions

□ Do not scan files larger than (KB): 8192
□ Stop if scan takes longer than (sec.) 60
☑ Do not ask for password when scanning objects

Objects scan acceleration

☑ Use the iStreams™ technology
NTFS file system alternate streams (ADS) are used during the scan.

☑ Use the iChecker™ technology
Scanned objects database is used during the scan.

Figure 39. Fine-tuning on-demand scan

In the **Objects scan acceleration** section you can enable or disable the use of the anti-virus scan acceleration technologies – iChecker™ and iStreams™ (for detailed description of these technologies see Appendix B on page 151). In order to use these technologies, check the corresponding boxes.

If, during the installation of the application, you disabled the use of the iStreams™ technology, in order to enable it, you will have to run the Kaspersky Anti-Virus installer again. Before you do it, you will not be able to configure the use of this technology.

7.3.2.2. Selecting an action to be performed with detected object

In the **Actions to be performed with detected objects** (see Figure 38) specify actions that Kaspersky Anti-Virus should perform each time it detects a dangerous or suspicious object.

- **Prompt user for action once the scan is completed** – suggest processing of dangerous objects detected when the scan is complete. This is a default mode and does not require your constant presence at the desk. Since this scan may take considerable time, we recommend using this mode when you cannot control processing dangerous objects as they are detected.
- **Prompt user for action during the scan** – ask user about the action to be performed on detected objects. A list of possible actions will be displayed, one of which will be recommended by Kaspersky Lab. Select this mode if you are staying at your computer during the scan.
- **Perform the recommended action** – perform the action recommended by Kaspersky Lab. Since the recommended actions are always well justified, you can select this mode in most cases. The recommended actions may be as follows:
    - *disinfect* infected objects;
    - *quarantine* suspicious or infected objects.

    Sometimes, after a file has been quarantined, a message appears notifying the user that the object cannot be deleted. This is related to the fact that quarantined objects are copied to the quarantine folder and deleted from their initial location. However, some objects (for instance, objects used by some programs) cannot be deleted in this way.

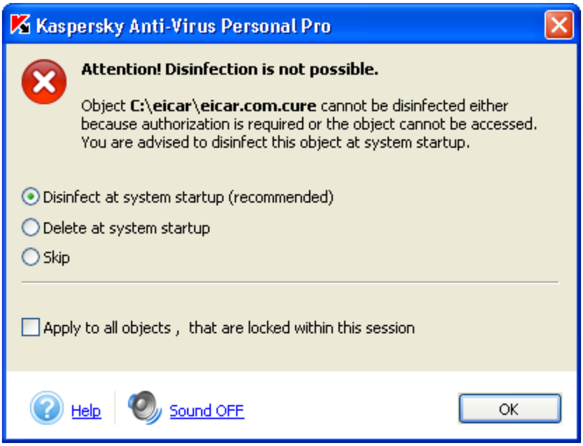
    - *delete* a dangerous object if it could not or cannot be disinfected.
- **Delete objects** – delete dangerous objects detected during the scan without making an attempt to disinfect them and without asking user's confirmation. When an object is deleted, its copy will be saved to the backup storage. This mode is recommended only if you are certain that you will not lose any valuable information.
- **Report only** – the application will only report infected and suspicious objects found during the scan but will not perform any action on such

objects. This mode is not recommended for most cases because all dangerous and other malicious objects will remain in your computer.

In some situations no action can be performed on an object, for instance, if an infected object is being used by another program at the time of deletion and therefore cannot be processed. In this case, a message will be displayed (see Figure 40) with a suggestion that you:

- *disinfect at system startup.* This action will be listed only if this object can be disinfected;
- *delete at system startup.* ;
- *skip* – do not perform any action on the object, only report its detection in the application report.

If you close the message window by clicking the ☒ button in the top right corner of the window, the action selected in this window will not be performed and the object will be skipped.


Kaspersky Anti-Virus Personal Pro

Attention! Disinfection is not possible.

Object **C:\eicar\eicar.com.cure** cannot be disinfected either because authorization is required or the object cannot be accessed. You are advised to disinfect this object at system startup.

● Disinfect at system startup (recommended)
○ Delete at system startup
○ Skip

□ Apply to all objects , that are locked within this session

Figure 40. Immediate object disinfection is impossible

For successful treatment (disinfection or deletion) of objects at system startup, the scan procedure during which such objects were detected must be fully completed. If you interrupt the scan procedure, such objects will not be disinfected/deleted.

7.4. Creating a list of exclusions

In some situations you may need to exclude some objects from the scope of the scan or real-time protection. You can also create such list of exclusions for on-demand scan tasks, real-time file protection tasks or real-time mail protection tasks.

The general list of all exclusions from the scope of the computer anti-virus protection can be viewed and edited in special window **Threats and exclusions** (see Figure 25).

In order to open this window, follow the Threats and exclusions link in the left part of the **Settings** tab (see Figure 6). The list of exclusions is created using the corresponding buttons.

*In order to add an exclusion, press the **Add** button.*

This will open the **Excluded object** window (see Figure 41) where you can specify the exclusion.

The following types of objects can be specified as exclusions:

- *Disks*, *folders*, *files*, *file masks*.
- *Threats* – types of malicious or potentially dangerous software.
- *Files associated with certain types of threats* – files that are assigned certain types of threats.

In order to exclude a certain folder or files (using file mask) from the scope of Kaspersky Anti-Virus protection,

Fill in the **Object** field using the … button.

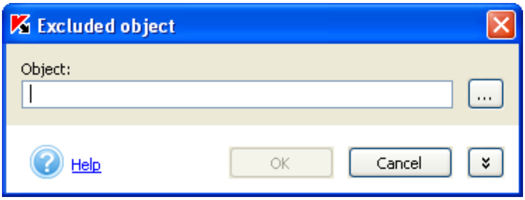


Figure 41. Creating list of exclusions

When you create the path to a folder to an object you can use the system environment variables. For example, you can select the Microsoft Windows operating system installation folder to be scanned by specifying %windir% as the variable.

When adding objects using mask, you can enter several masks at the same time separating them with a space. If the filename contains spaces, such filename must be specified in quotes.

Listed below are examples of allowed exclusion masks:

- Masks used without specifying the path to objects:
  - ***.exe** – all files with extension exe
  - ***.ex?** – all files with extension ex?
  - **test** – all files with filename test
- Masks used with absolute paths to objects:
  - **C:\dir\*.*** – all files in folder C:\dir\
  - **C:\dir\*.exe** – all files with extension exe in folder C:\dir\
  - **C:\dir\*.ex?** – all files with extension ex? in folder C:\dir\
  - **C:\dir\test** – file C:\dir\test only
  - **C:\dir\** – all files in folder C:\dir\ including all subfolders
- Masks used with relative paths to objects:
  - **dir*.*** – all files in all folders under dir\
  - **dir\test** – all files with filename test in folders under dir\
  - **dir*.exe** – all files with extension exe in all folders under dir\
  - **dir*.ex?** – all files with extension ex? in all folders under dir\
  - **dir** – all files in all folders under dir\ and in all their subfolders

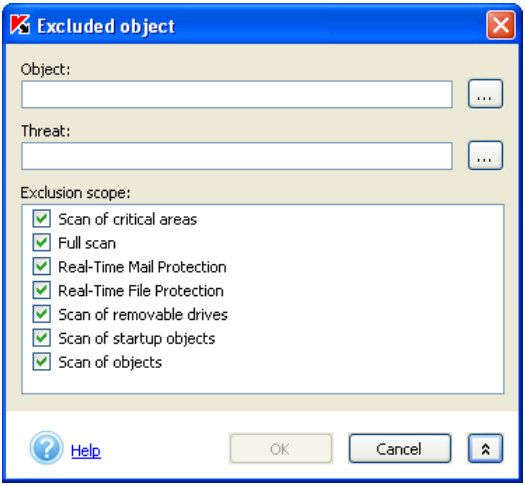
We do not recommend to enter ***.*** and ***** masks as these masks are equivalent to disabling the real-time protection.

We do not recommend selecting as exclusion a virtual drive created based on the file system folder using the subst command. This does not make sense as when performing a scan, Kaspersky Anti-Virus will treat this virtual drive as a folder and, therefore, will scan it.

In order to exclude from the anti-virus processing scope all files that were assigned a certain threat type as a result of an anti-virus scan,

open the additional part of the window (see Figure 42) by pressing button ⌄ and select the threat type in **The list of detectable threats** dialog box (see Figure 43) that opens by clicking button ….

In this window you can search for a threat by a part of its name, sort the list of threats by clicking the heading of the **Name** column and copy the name of a threat into the buffer using the corresponding command of the shortcut menu. You can also view the detailed description of a threat at www.viruslist.com. In order to do it, select the threat in the list and use the **Details** command of the shortcut menu.



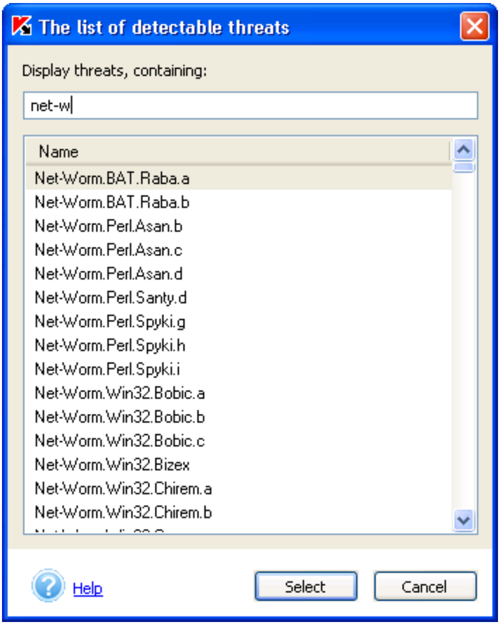
Object:

Threat:

Exclusion scope:

- ☑ Scan of critical areas
- ☑ Full scan
- ☑ Real-Time Mail Protection
- ☑ Real-Time File Protection
- ☑ Scan of removable drives
- ☑ Scan of startup objects
- ☑ Scan of objects

Figure 42. Creating list of exclusions



Display threats, containing:

net-w

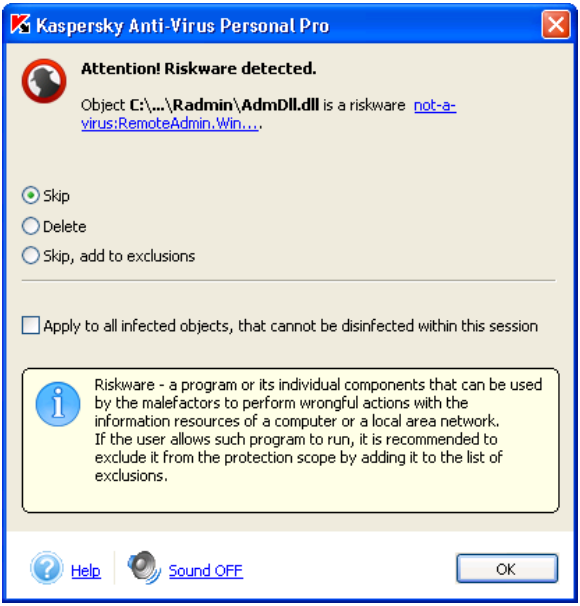
Name
Net-Worm.BAT.Raba.a
Net-Worm.BAT.Raba.b
Net-Worm.Perl.Asan.b
Net-Worm.Perl.Asan.c
Net-Worm.Perl.Asan.d
Net-Worm.Perl.Santy.d
Net-Worm.Perl.Spyki.g
Net-Worm.Perl.Spyki.h
Net-Worm.Perl.Spyki.i
Net-Worm.Win32.Bobic.a
Net-Worm.Win32.Bobic.b
Net-Worm.Win32.Bobic.c
Net-Worm.Win32.Bizex
Net-Worm.Win32.Chirem.a
Net-Worm.Win32.Chirem.b

Figure 43. List of detectable threats

In order to exclude a certain object with a known threat type from the scan scope,

1. Specify the object's name in the **Object** field.
2. Enter the threat type in the **Threat** field.

You can also exclude file with a certain threat type using a notification that opens when Kaspersky Anti-Virus has detected such file (see Figure 44).



Kaspersky Anti-Virus Personal Pro

Attention! Riskware detected.

Object **C:\...\Radmin\AdmDll.dll** is a riskware not-a-virus:RemoteAdmin.Win....

● Skip
○ Delete
○ Skip, add to exclusions

□ Apply to all infected objects, that cannot be disinfected within this session

Riskware - a program or its individual components that can be used by the malefactors to perform wrongful actions with the information resources of a computer or a local area network.
If the user allows such program to run, it is recommended to exclude it from the protection scope by adding it to the list of exclusions.

Figure 44. Threat notification

Additionally, you can determine the task to which Kaspersky Anti-Virus will apply the specified exclusion. Check boxes in the **Exclusion scope** section for those task to which the exclusions should apply. The list includes: the scan or high risk areas, full computer scan, real-time mail protection, real-time file protection and on-demand scan tasks (both system and user-defined tasks).

7.5. Monitoring software processes

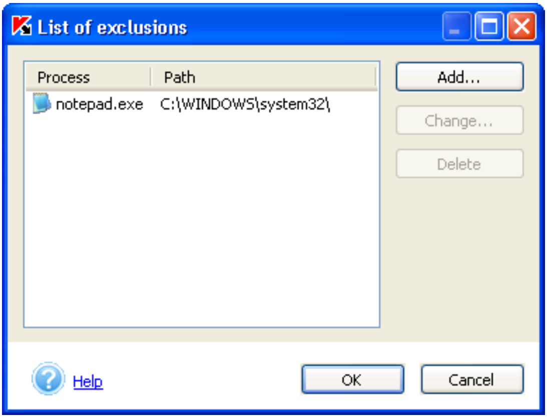
Kaspersky Anti-Virus allows creation of the list of software processes that will not be monitored by the application in the real-time protection mode.

For example, you think that objects used by the **Notepad**, a standard Microsoft Windows application, are safe and do not require real-time protection scan. In other words, you trust the process of this program. In order to exclude objects used by this process from the scan scope, add the **Notepad** application to the list of trusted processes.

In order to create a list of trusted processes,

Follow the specified/not specified link next to the **Trusted processes** setting in the **Protection level settings** section on the **Files** tab (see Figure 25)

This will open the **List of exclusions** window (see Figure 45). You can fill or edit the list using buttons to the right of the list.



Process	Path
notepad.exe	C:\WINDOWS\system32\

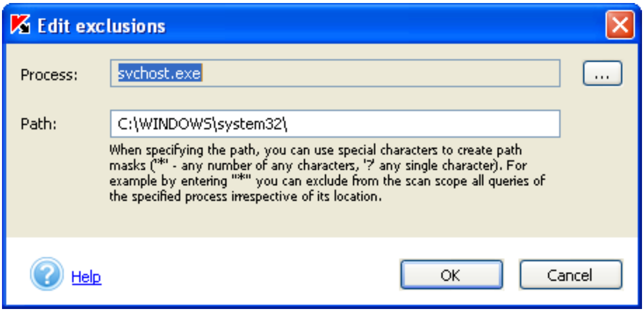
Figure 45. Creating a trusted processes list

Using the **Add** button, you can add to the list of exclusion:

- *an executable file*. To do this, use the **Browse** command and specify the corresponding **.exe** file;
- *a running process*. In order do to this, use the **Running process** command and select one of the running processes in the list that will open.

In order to remove a process from the list, specify the required process and press the **Delete** button.

When the **Edit...** button is pressed, an additional window opens (see Figure 46).



Process: svchost.exe

Path: C:\WINDOWS\system32\

When specifying the path, you can use special characters to create path masks ("*" - any number of any characters, '?' any single character). For example by entering "*" you can exclude from the scan scope all queries of the specified process irrespective of its location.

Figure 46. Editing a trusted processes

The process filename can be changed using the ... button. When you select the name, Kaspersky Anti-Virus remembers the internal attributes of the process files that it uses to identify the process as trusted during the scan.

Path to the file will be provided automatically when the name is selected. You can modify it manually later.

Path shall be specified as full path to the process file or as a mask * (any number of any characters) or **?** (any one character).

For example, when using mask *, the running process will be considered trusted irrespective of the process file location folder.

7.6. Creating a task launch schedule

You can create a schedule for automatic launch of on-demand scan and updating tasks. This will ensure that you timely receive updated anti-virus database and perform regular scan of the objects stored in your computer.

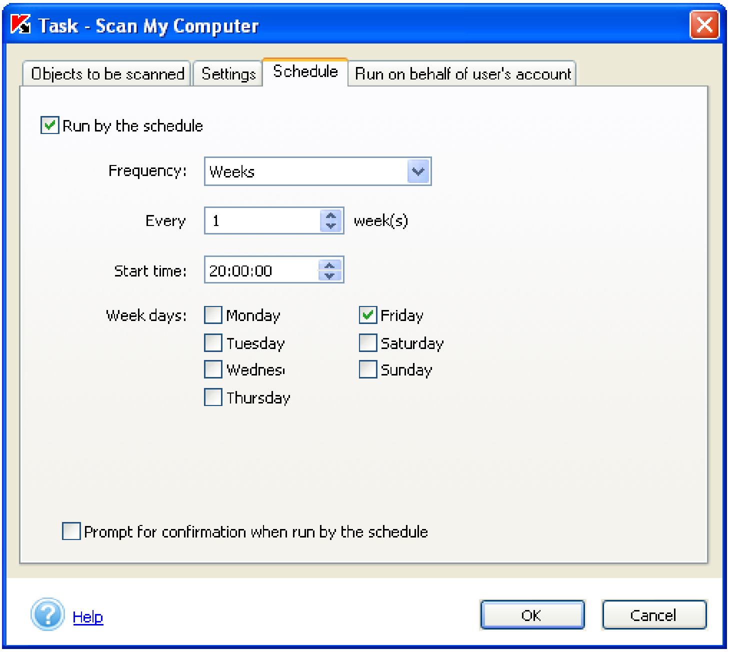
By default Kaspersky Anti-Virus updates anti-virus database every three hours and performs a full computer scan every Friday at 8:00 pm.

In order to modify the anti-virus database updating schedule,

use the Configure Updater link located in the left part of the **Settings** tab. This will open an updater settings window on the **Update** tab (see Figure 19).

In order to create/modify an on-demand scan tasks schedule,

1. Follow the On-Demand Scan tasks link located in the left part of the **Settings** tab (see Figure 6).
2. In the list of the scan tasks (see Figure 35) select task for which you wish to create/modify the schedule and press the **Properties** button. This will open window where you can fine-tune this task (see Figure 36). The schedule can be configured in the **Schedule** tab (see Figure 47).



☑ Run by the schedule

Frequency: Weeks

Every 1 week(s)

Start time: 20:00:00

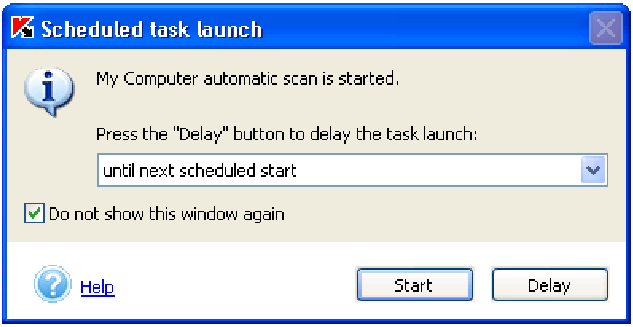
Week days: □ Monday ☑ Friday
□ Tuesday □ Saturday
□ Wednes □ Sunday
□ Thursday

□ Prompt for confirmation when run by the schedule

Figure 47 . Configuring schedule

In order to enable an automatic scheduled task launch, check the ☑ **Run by the schedule** box.

If you would like to receive notifications about the upcoming update, check the ☑ **Prompt for confirmation when run by the schedule** box. If this box is checked, the **Scheduled task launch** window will be displayed before such scheduled task is run (see Figure 48). Press the **Start** button in order to start a scheduled scan. In order to postpone the scan for some time, select the required time interval from the drop-down list and press the **Delay** button. If the user takes no action in the prompt window within 3 minutes, the task will be started automatically.



Scheduled task launch

My Computer automatic scan is started.

Press the "Delay" button to delay the task launch:

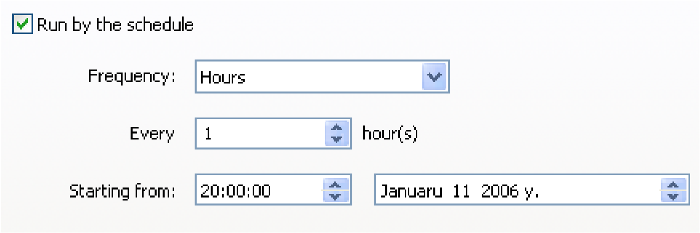
until next scheduled start

☑ Do not show this window again

Figure 48 . Configuring schedule

Select the interval for the task execution in the **Frequency** field. The following options are provided: hours, days, weeks, at the application startup. Depending on the option selected, the central part of the window with date entry fields will change its appearance:

- *Hours*: the task is launched on a schedule with the frequency of several hours. Specify the frequency (in hours).



☑ Run by the schedule

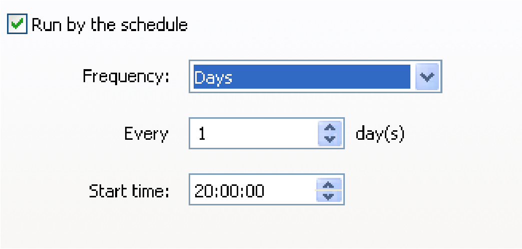
Frequency: Hours

Every 1 hour(s)

Starting from: 20:00:00 Januaru 11 2006 y.

Figure 49 . Configuring schedule (frequency in hours)

- *Days*: the task is launched with the interval of several days. Specify the frequency in days (in days) and the launch time.



☑ Run by the schedule

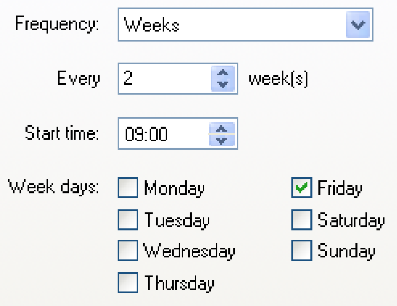
Frequency: Days

Every 1 day(s)

Start time: 20:00:00

Figure 50. Configuring schedule (frequency in days)

- *Weeks*: the task is launched with the interval of several weeks. Specify the frequency (in weeks), select the week day and the launch time.



Frequency: Weeks

Every 2 week(s)

Start time: 09:00

Week days: □ Monday □ Tuesday □ Wednesday □ Thursday ☑ Friday □ Saturday □ Sunday

Figure 51. Configuring schedule (frequency in weeks)

- *At the program startup*: the task will be launched immediately after Kaspersky Anti-Virus is started.

7.7. Running a task on behalf of another user's account

Running Kaspersky Anti-Virus tasks on behalf of a privileged user may be required when there are several users having different rights have access to your computer.

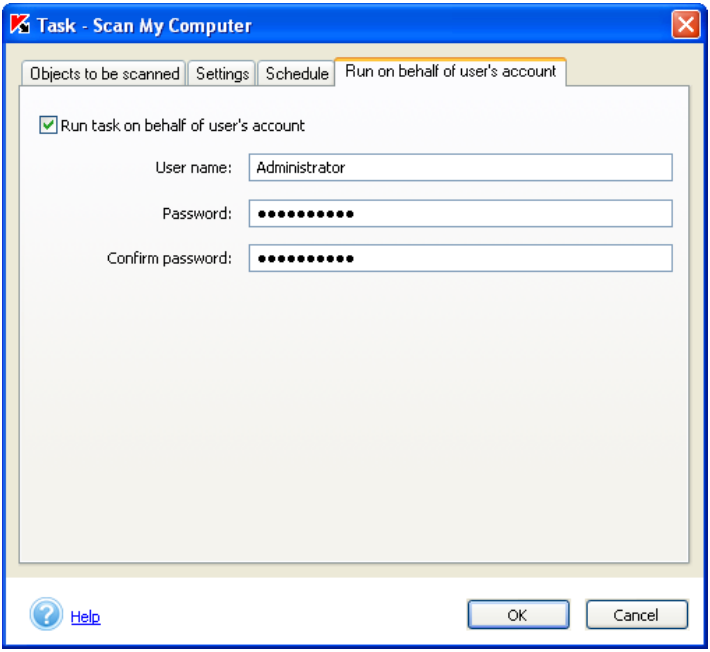
When using the service, the computer administrator enters the information for the profile that has sufficient rights to access a certain object. For instance, running an on-demand scan task requires access rights to the objects scanned while running an update task requires an access right to updates folder or the rights of an authorized user of a proxy server.

This allows avoiding mistakes when running on-demand scan tasks and updates tasks when the user running a task, does not have sufficient access rights.

By default this service is disabled and tasks are launched on behalf of the current profile. You can enable the function of running updates or on-demand scan tasks on behalf of a different profile using the **Run on behalf of user's account** tab (see Figure 52) in the settings dialog box of updater or on-demand scan task configuration.

In order to do this check the ☑ **Run task on behalf of user's account** box.

Enter the profile information (username and password) below the profile on which behalf the task will be run:



Task - Scan My Computer

☑ Run task on behalf of user's account

User name: Administrator

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Figure 52. Configuring running task on behalf of another user's account

CHAPTER 8. ADDITIONAL FUNCTIONALITY

Kaspersky Anti-Virus offers the following additional functions that may be used to configure and run the application, such as:

- Configuring quarantine and backup storage
- Managing quarantined objects.
- Managing backup copies of objects.
- Application report analysis.
- Managing Kaspersky Anti-Virus configuration
- Additional settings
- Notifications configuration
- Work in the administrator's and in the user's mode

This chapter contains a detailed discussion of each of the above options.

8.1. Configuring quarantine and backup storage settings

You can customize the settings for the creation and operation of the quarantine and of the backup storage. To configure the quarantine settings, click Configure Quarantine&Backup on the **Settings** tab (see Figure 6) of the main application window.

Edit the following parameters (see Figure 53) in the corresponding section (quarantine or backup storage) of window that will open:

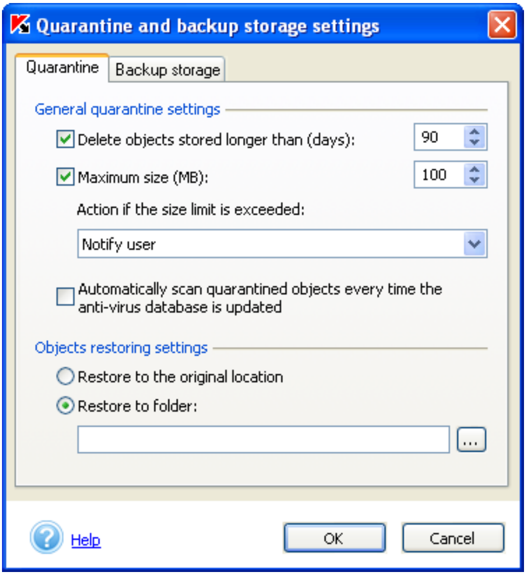
☑ **Delete objects stored longer than (days)**. By default, the storage time of quarantined files is not limited. You can limit this period by checking the corresponding box and specifying the number of days in the corresponding spin-button box (the default value is 90 days).

☑ **Maximum size (MB)**. By default, the quarantine size is not limited. If you wish to restrict the total size of the files in the storage, check the corresponding box and specify the size using the up and down arrows of the corresponding spin-button box (the default value is 100 MB). Select the action that will be performed by the Kaspersky Anti-Virus in case the storage size is exceeded:

- *Notify user* - when the quarantine size is exceeded, a prompt for action will be displayed;
- *Delete older objects* - delete files that had been quarantined earlier than others.

☑ **Automatically scan quarantined objects every time the anti-virus database is updated**. This mode of Kaspersky Anti-Virus provides for an automatic scan of the quarantined objects each time the anti-virus database gets updated.

⚠ Kaspersky Anti-Virus will not be able to scan quarantined objects immediately after you updated your anti-virus database if you were working with the quarantine at the time of update.



Quarantine and backup storage settings

Quarantine | Backup storage

General quarantine settings

☑ Delete objects stored longer than (days): 90

☑ Maximum size (MB): 100

Action if the size limit is exceeded:

Notify user

☐ Automatically scan quarantined objects every time the anti-virus database is updated

Objects restoring settings

○ Restore to the original location

● Restore to folder:

Figure 53. Configuring quarantine settings

Specify the location where objects will be restored in the **Objects restoring settings** section:

● **Restore to the original location**. By default restored copies will be saved to the location where Kaspersky Anti-Virus detected the infected object.

● **Restore to folder**. If this option is selected, you will have to specify the path to the folder into which restored objects will be saved.

Such settings as maximum size of the backup storage and terms of storage and restoration of the backup copies of objects are the same as for the quarantine.

8.2. Working with quarantined objects

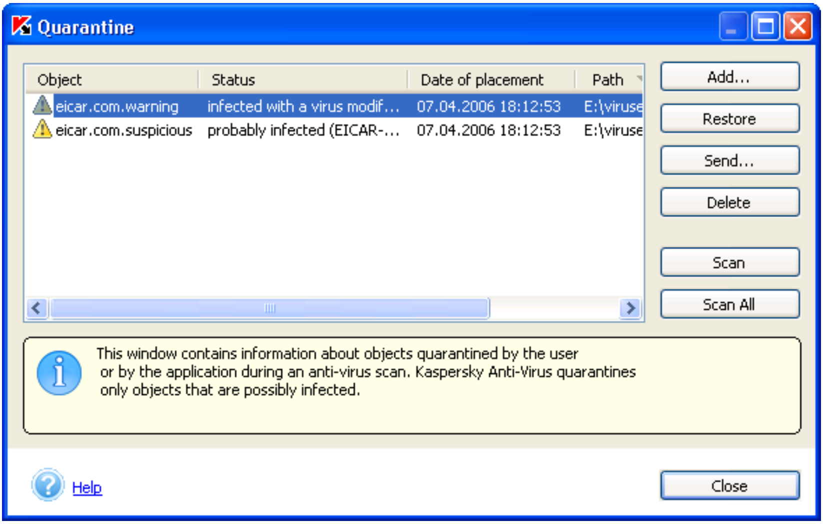
During the scan of the entire computer, disks or files or when the real-time protection is enabled, Kaspersky Anti-Virus places all objects that are possibly detected with viruses or their modifications into the quarantine folder where you can proceed working with them (rescan, restore, delete, etc.). The quarantined files are stored in a special format and do not impose any threat.

A heuristic code analyzer, detecting up to 92% of new viruses, determines whether a file is suspicious in terms of possible presence of a virus. This mechanism is quite effective and cases of false positives are extremely rare.

We recommend that you update the anti-virus database before scanning quarantined files. The update may contain information about any viruses which have infected the quarantined files, and you may be able to repair the files.

You can work with possibly infected files in the **Quarantine** window (see Figure 54), which can be opened by clicking View Quarantine in the **Protection** tab (see Figure 5) of the main application window or by clicking the View Quarantine link in the **Scan** window (see Figure 8).

The total number of quarantined objects is displayed in brackets next to the Quarantine link on the **Protection** tab.



Quarantine

Object	Status	Date of placement	Path
eicar.com.warning	infected with a virus modif…	07.04.2006 18:12:53	E:\viruse
eicar.com.suspicious	probably infected (EICAR-…	07.04.2006 18:12:53	E:\viruse

This window contains information about objects quarantined by the user or by the application during an anti-virus scan. Kaspersky Anti-Virus quarantines only objects that are possibly infected.

Figure 54. Quarantined possibly infected files

The following actions can be performed from the **Quarantine** window:

- Quarantine a file suspected of being infected with a virus that is not detected by Kaspersky Anti-Virus. To quarantine a file, click **Add** and select the suspicious file in the standard file selection window. The file will be added to the list with the status quarantined by user.

- Scan and disinfect all of, or a subset of, the suspicious files using the current anti-virus database. To do this, either click **Scan All**, or select the files to be scanned and click **Scan**.

  After the scanning and disinfection of a quarantined object its status may change to *infected, false alarm*, *not infected,* etc. In this case, a message will give recommendations on how to treat with this file.

  The *infected* status means that the object was identified as dangerous but its disinfection failed. We recommend that you delete such objects.

  All objects with the *false alarm* status may be safely restored, as their previous *possibly infected* status was not confirmed by Kaspersky Anti-Virus.

You can run the **Scan quarantine** task in the **On-Demand scan tasks** window (see Figure 34). When the task is started, the **Scan** window (see Figure 8) will be displayed on the screen. The scan results can be viewed in the report (details see section 8.4 on page 114).

The **Scan Quarantine** task is similar to the task launched using the **Scan All** button in the Quarantine window (see Figure 54).

- Restore files from the quarantine folder to their original folders. To restore an object, select it in the list and click the **Restore** button. When restoring objects quarantined from archives, email databases and mail format files, you must specify the folder to which they are to be restored.

We recommend that you restore only objects with a *false alarm, not infected* or *disinfected* status because restoring other objects may infect your computer!

- Send suspicious objects to Kaspersky Lab for analysis. We recommend that you only send objects that have retained their possibly infected status after numerous attempts to scan and disinfect them. To send a file to Kaspersky Lab, click **Send** (for details see section Chapter 11 on page 143).

Note that files that you send to Kaspersky Lab for analysis should be scanned by Kaspersky Anti-Virus, using an anti-virus database updated at most one day before you send the file.

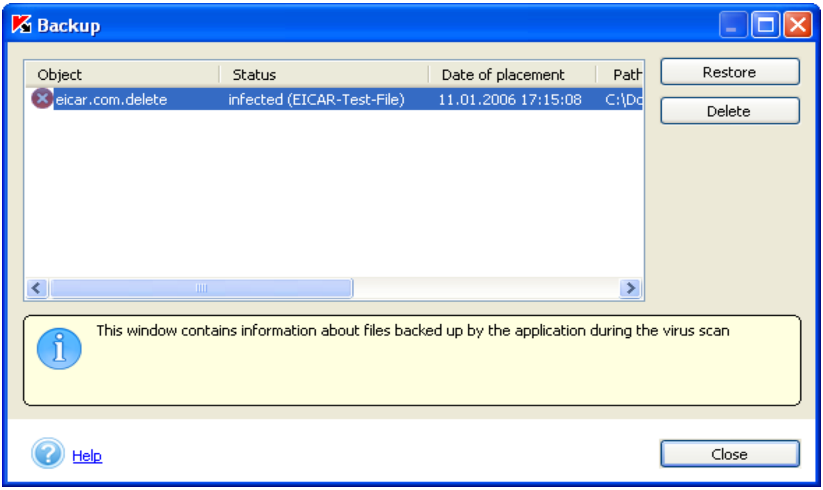
- Delete a quarantined object or a selected group of objects. Delete only files that cannot be disinfected. To delete such files, select them in the list and click the **Delete** button.

8.3. Working with backup copies of objects

Backup storage is a special storage area used to store backup copies of objects. Backup copies are created when an object is attempted to be disinfected or deleted for the first time. The major function of the backup storage - to keep these copies so that the initial object can be restored at any moment.

You can manage backup copies via a dialog window **Backup** (see Figure 55). In order to access this window, follow the View Backup link in the left section of the **Protection** tab (see Figure 5).

The total number of objects copies placed in the backup storage is displayed in brackets next to the Backup storage link on the **Protection** tab.



Object	Status	Date of placement	Path
eicar.com.delete	infected (EICAR-Test-File)	11.01.2006 17:15:08	C:\Dc

This window contains information about files backed up by the application during the virus scan

Figure 55. Backup storage

The central part of the window contains the list of backup copies. The following information is provided for each copy: name of the object for which the copy is created, object status, copy creation date and the full path to the initial object's location.

You can restore or delete a copy or several selected copies using the corresponding buttons to the right of the list.

Object is restored from the backup copy under the same name it had before processing.

If an object with the same name is found at the initial location (this is possible if you are restoring an object that was backed up and then disinfected), the corresponding warning will be displayed. You may select a different location for the object being restored or rename the object.

When is it safe to restore backup copies?

When disinfecting objects, their integrity sometimes can not be maintained. If the disinfected file contained important information that have become completely or partly unavailable, you can try to restore the initial object from the backup copy. We recommend that you scan such objects for viruses immediately after their restoration as such object may be successfully disinfected without data loss using updated anti-virus database.

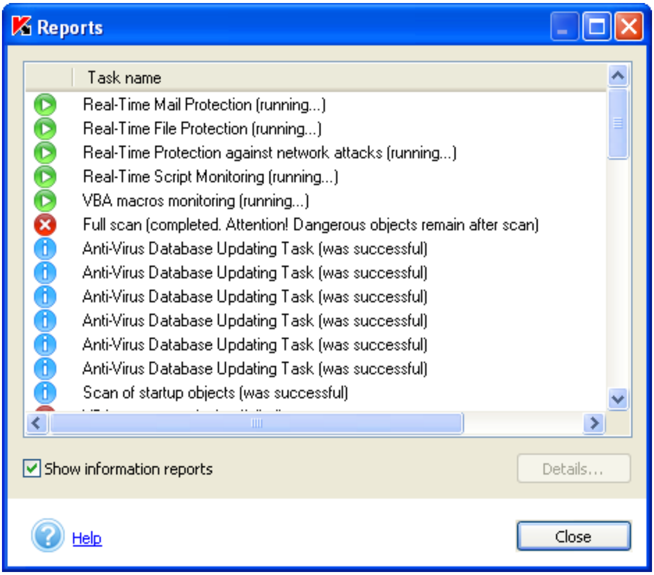
We do not recommend to restore objects from backup copies, if it is not necessary as this may result in an infection of your computer.

By default the period of storing such backup copies and the maximum size of the backup storage are not limited. We recommend that you periodically view and clean the backup storage. You may also setup the program so that it automatically removes older copies and notifies you about the backup storage overflow (for details see section 8.1 on page 108)

8.4. Working with reports

The application maintains reports during anti-virus scans, while the anti-virus database is updating and while real-time protection is enabled. The reports include information about the objects scanned, processing results and general statistical data.

A complete list of all reports about tasks performed or being performed by Kaspersky Anti-Virus can be viewed in the **Reports** windows (see Figure 56). You can open this window by clicking the View reports hyperlink in the left section of the **Protection** tab (see Figure 5).



Task name
Real-Time Mail Protection (running...)
Real-Time File Protection (running...)
Real-Time Protection against network attacks (running...)
Real-Time Script Monitoring (running...)
VBA macros monitoring (running...)
Full scan (completed. Attention! Dangerous objects remain after scan)
Anti-Virus Database Updating Task (was successful)
Anti-Virus Database Updating Task (was successful)
Anti-Virus Database Updating Task (was successful)
Anti-Virus Database Updating Task (was successful)
Anti-Virus Database Updating Task (was successful)
Anti-Virus Database Updating Task (was successful)
Scan of startup objects (was successful)

☑ Show information reports

Figure 56. Reports

The following report types are provided:

- ▶ or ℹ – *Information reports* contain reference information (for example, the task started, the task completed, the task is in progress, the task is paused).
- ✖ – *“Attention” reports* contain critical information (for example, Attention! Untreated objects remain).
- ⚠ – *“Note" reports* comment on important issues of the application’s operation (for example, the task was interrupted).

As a rule, information reports are provided for reference only and are of no special interest. The display of information messages can be disabled by unchecking the ☑ **Show information reports** box. Note that reports about tasks currently in progress, indicated by icon ▶, will always be displayed.

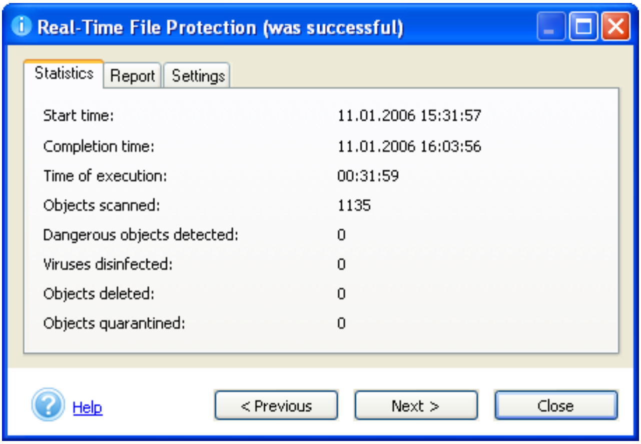
Reports can be sorted by report type, by title (in alphabetical order) and by task completion time. To sort the reports by any of the above columns, simply click the header of the corresponding column.

To view the settings, statistics and outcome of a specific task listed in the log, select the task and click the **Details** button, or double-click the task.

This will open a new window with a detailed report on the task in the **Statistics**, **Report**, and **Settings** tabs.

While running on-demand scan tasks, you can monitor the task performance in the same way (see Figure 8).

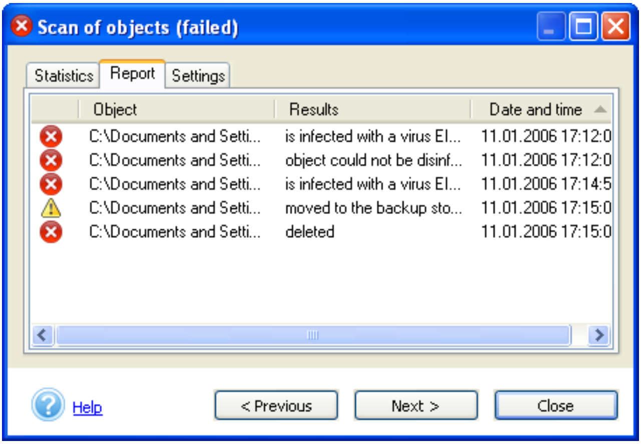
For scanning tasks, the **Statistics** tab displays general information about the work performed by Kaspersky Anti-Virus to implement the task, including: the date and time the task was started, the total number of files scanned and the number of infected, disinfected and quarantined objects (see Figure 57). For the update task this tab will display the total size of the update files at the source and the total size of files downloaded to your computer.



Start time:	11.01.2006 15:31:57
Completion time:	11.01.2006 16:03:56
Time of execution:	00:31:59
Objects scanned:	1135
Dangerous objects detected:	0
Viruses disinfected:	0
Objects deleted:	0
Objects quarantined:	0

Figure 57. The **Statistics** tab

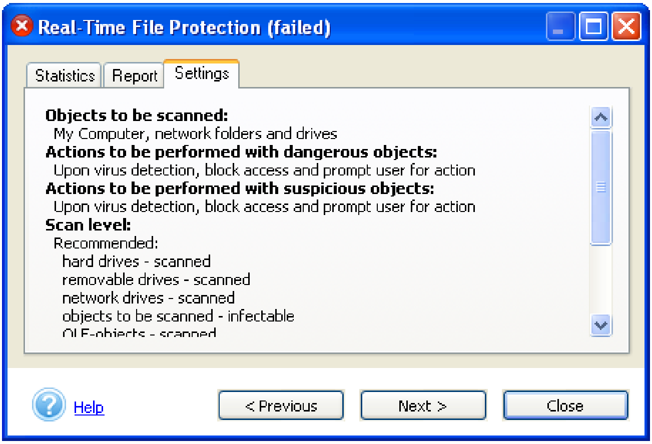
For scanning tasks, the **Report** tab (see Figure 58) by default only displays information about viruses detected. To display information about uninfected files as well, check the ☑ **Log all reports** box in the **Additional Settings** window of Kaspersky Anti-Virus (see section 8.6 on page 120). If you do so, the **Report** tab will contain information on each scanned object. For the update task this tab displays information on each step: on establishing connection with the updates source, about the downloaded files, and installation information. For the update task this information will always be displayed irrespective of whether or not the ☑ **Log all reports** box in the **Additional Settings** window is checked.



	Object	Results	Date and time
☒	C:\Documents and Setti...	is infected with a virus EI...	11.01.2006 17:12:0
☒	C:\Documents and Setti...	object could not be disinf...	11.01.2006 17:12:0
☒	C:\Documents and Setti...	is infected with a virus EI...	11.01.2006 17:14:5
⚠	C:\Documents and Setti...	moved to the backup sto...	11.01.2006 17:15:0
☒	C:\Documents and Setti...	deleted	11.01.2006 17:15:0

Figure 58. The **Report** tab

For tasks, the **Settings** tab (see Figure 59) displays parameters used by the task including information about the objects scanned, protection level applied to this task and actions to be performed with suspicious and infected objects.



Objects to be scanned:
My Computer, network folders and drives
Actions to be performed with dangerous objects:
Upon virus detection, block access and prompt user for action
Actions to be performed with suspicious objects:
Upon virus detection, block access and prompt user for action
Scan level:
Recommended:
hard drives - scanned
removable drives - scanned
network drives - scanned
objects to be scanned - infectable
OLE-objects - scanned

Figure 59. The **Settings** tab

This information also includes the list of exclusions from the scan scope if such exclusions have been specified. For update tasks the update type and update source are displayed.

You can select the tasks to be viewed in the **Reports** windows or in the detailed task report dialog box using the **Next >** and the **< Previous** buttons.

8.4.1. Displaying reports

Kaspersky Anti-Virus allows you to choose which information will be displayed in reports. You may configure the application so that only important information will be recorded in reports, while information and other reference messages will not be entered.

You can enable logging all reports by checking the ☑ **Log all reports** in the **Additional Settings** window (see section 8.6 on page 120). You may view all messages displayed for instance when you start a full computer scan in the Scan window (see Figure 8) in the **Report** tab.

If this box is checked, a detailed report about the task performed will be compiled, including information about the correct processing of the object.

If the box is unchecked, only “attention” reports and “note” reports will be displayed: for example a message that an object has not been scanned due to an error. Messages about successful processing will not be displayed.

To disable displaying information reports within the current session without unchecking the ☑ **Log all reports** box,

right-click the window while viewing reports in the **Report** tab to open a shortcut menu (see Figure 60) and uncheck the **Show detailed report** flag.

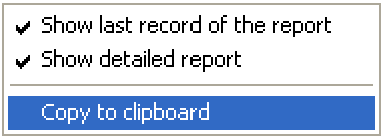


Figure 60. Shortcut menu

If the ☑ **Log all reports** box in the **Additional Settings** window is unchecked, the **Show detailed report** option in the context menu will also be unchecked and disabled and you will not be able to configure displaying information reports.

When you are viewing the report in the monitoring mode (i.e. during the scan in the **Report** tab), by default you will always see the last record of the report. To disable this mode, right-click to open shortcut menu and uncheck the **Show last record of the report** box or simply select a record in the report.

You can also copy information about an individual even into the clipboard. In order to do this, select the events you are interested in and use the **Copy to Clipboard** command from the shortcut menu.

8.4.2. Exporting and sending reports

Kaspersky Anti-Virus allows you to edit the list of reports created based on the results of various tasks. You may access available editing options from the context menu (see Figure 61), which you can open by right-clicking the **Report** window (see Figure 56).

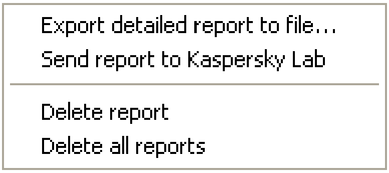

Export detailed report to file...
Send report to Kaspersky Lab
Delete report
Delete all reports

Figure 61. Shortcut used for managing reports

You cannot delete a report while the task creating the report is in progress.

Exporting a detailed report to a file allows you to view its contents in the form of a Microsoft Excel table or a plain text file.

If any task (for instance, a computer scan or anti-virus database updating process) is interrupted or results in an error and you do not know what caused this application behavior, you may send a report on the task to Kaspersky Lab.

To do this, select the report you wish to send in the **Reports** window, right-click the selected report and choose the **Send report to Kaspersky Lab** option in the shortcut menu. This will open a new window of your default email client application (for example, Microsoft Outlook Express) containing a new email message with the report file attached to it. Send this message and Kaspersky Lab will respond to it as soon as possible.

Mail messages are automatically created using exclusively Microsoft Office Outlook or Microsoft Outlook Express. If you have a different mail program installed on your computer (for instance, TheBat!), you will have to configure your mail program's Simple MAPI to ensure that automatic message creation is supported.

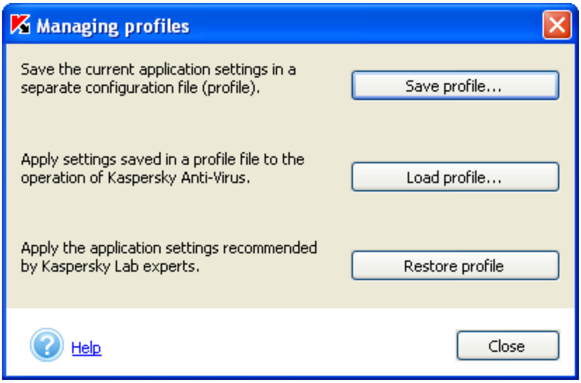
8.5. Managing Kaspersky Anti-Virus configuration

Kaspersky Anti-Virus allows the user to create and use various configurations in its operation. Now you can configure a certain mode of the programs' operation, save its settings in a special configuration file (profile) and use this configuration when it is needed.

In order to access the program configuration tools, follow the **Managing profiles** hyperlink in the left part of the **Settings** tab (see Figure 6).

You can save the current application settings in a special configuration file by pressing the **Save profile…** button in the window that will open (see Figure 62) or apply the settings of any configuration created earlier by pressing the **Load profile...** button. Since some modes of operation can be activated only when the operating system is started, a system restart may be required when you load some settings.

In order to restore the recommended settings, press the **Restore profile** button.



Managing profiles

Save the current application settings in a separate configuration file (profile).

Apply settings saved in a profile file to the operation of Kaspersky Anti-Virus.

Apply the application settings recommended by Kaspersky Lab experts.

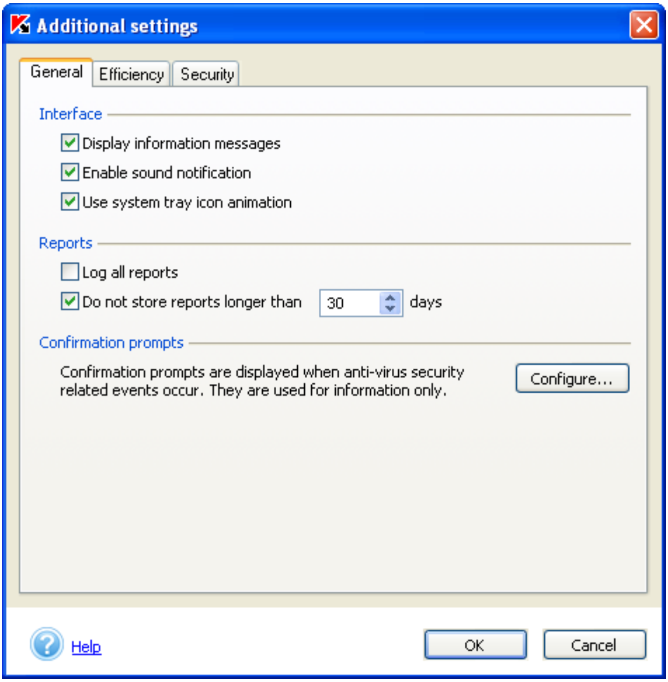
Figure 62. Managing Kaspersky Anti-Virus Personal Pro profiles

8.6. Additional settings of Kaspersky Anti-Virus Personal Pro

In addition to configuring the settings for particular tasks, Kaspersky Anti-Virus Personal allows configuration of some general and service settings (see Figure 63).

In order to configure additional Kaspersky Anti-Virus settings,

Follow the Additional Settings hyperlink in the left part of the **Settings** tab (see Figure 6). This will open a dialog box containing the **General**, **Efficiency** and **Security** tabs.



Additional settings

Interface

☑ Display information messages

☑ Enable sound notification

☑ Use system tray icon animation

Reports

☐ Log all reports

☑ Do not store reports longer than 30 days

Confirmation prompts

Confirmation prompts are displayed when anti-virus security related events occur. They are used for information only.

Figure 63. Additional settings of Kaspersky Anti-Virus Personal Pro
The **General** tab

Using the **General** tab (see Figure 63) you can configure the following settings:

- ☑ **Display information messages** – enable the display of all pop-up tips accompanying the operation of Kaspersky Anti-Virus. You are advised not to disable this mode because the application often operates in interactive mode requiring the user's feedback when processing objects.

  Microsoft Windows 98 and Microsoft Windows NT Workstation 4.0 operating systems do not support displaying of informational messages.

- ☑ **Enable sound notification** – enable sound effects accompanying some events occurring displayed during Kaspersky Anti-Virus operation. You can view the list of events or modify the set of the audio files corresponding to such events using standard Windows tools **Start → Settings → Control Panel → Sounds and Audio Devices → Sounds**.

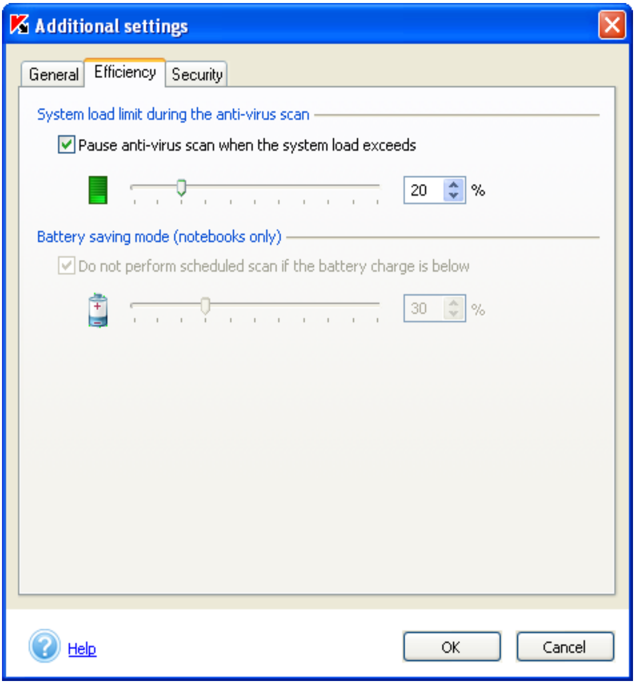
- ☑ **Use system tray icon animation** – enable the icon animation depending on the task performed by Kaspersky Anti-Virus. For example, a blinking envelope above the icon indicates that the application is scanning an e-mail message.

☑ **Log all reports** – enable recording of all reports, created during the program operation: information messages, error notifications, etc. By default, this mode is disabled and only important reports are logged, such as program's completion with an error, interruption of a task execution, etc.

☑ **Do not store reports longer than ... days** – by default, reports are kept for thirty days. This period may be changed by entering a value in the field on the right side. To remove this restriction, uncheck the corresponding box. While the application is loading, a check for reports stored longer than the specified period will be performed and obsolete reports will be deleted.

The **Confirmation prompts** section allows the user to control displaying notifications about certain events in the operation of Kaspersky Anti-Virus. As a rule, all notifications are displayed for user's reference. For more details about configuring the confirmation prompts see section 8.7 on page125).

Using the **Efficiency** tab (see Figure 64) you can configure restrictions imposed on the on-demand scan in order to save the battery charge (if you are using a notebook) and the operating system's resources (details see section 8.8 on page 126).


Additional settings

System load limit during the anti-virus scan

☑ Pause anti-virus scan when the system load exceeds 20 %

Battery saving mode (notebooks only)

☑ Do not perform scheduled scan if the battery charge is below 30 %

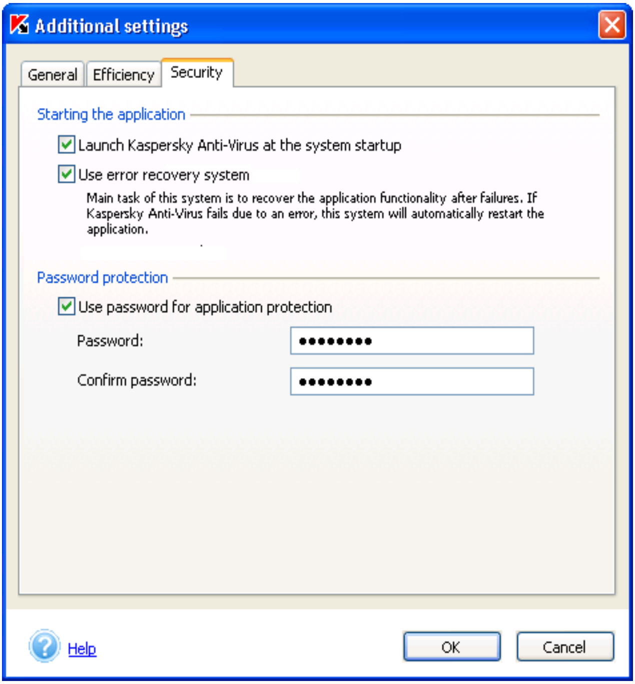
Figure 64. Additional settings of Kaspersky Anti-Virus Personal Pro
The **Efficiency** tab

Using the **Security** tab (see Figure 66) you can configure the following settings:

☑ **Launch Kaspersky Anti-Virus at the system startup** – enable the automatic launch of Kaspersky Anti-Virus when the operating system is restarted.

We strongly recommend that you do not disable the automatic launch of Kaspersky Anti-Virus because this increases the risk of your computer becoming infected.

You cannot modify this setting if you do not have Administrator's rights for this computer.



Starting the application

☑ Launch Kaspersky Anti-Virus at the system startup

☑ Use error recovery system

Main task of this system is to recover the application functionality after failures. If Kaspersky Anti-Virus fails due to an error, this system will automatically restart the application.

Password protection

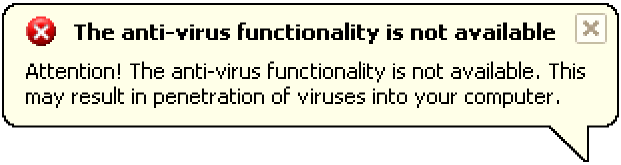
☑ Use password for application protection

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Figure 65. Additional settings of Kaspersky Anti-Virus Personal Pro. The **Security** tab

☑ **Use error recovery system** – enable Kaspersky Anti-Virus operation recovery after a failure. If the operation of the application was interrupted, the main Kaspersky Anti-Virus window will be minimized (if it was open) and an information message will appear above the icon the in the system tray (see Figure 66). After this the application will recover automatically.



The anti-virus functionality is not available

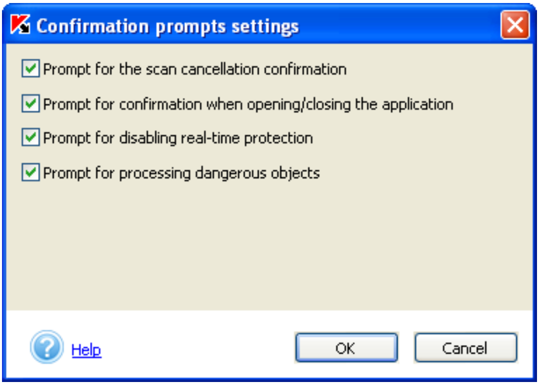
Attention! The anti-virus functionality is not available. This may result in penetration of viruses into your computer.

Figure 66. Application failure

☑ **Use password for application protection** – enable prompting for password when switching to the administrator's mode. We recommend that you use this mode if there are other users who have access to your computer whom you do not want to alter your anti-virus protection settings, disable the real-time protection or close Kaspersky Anti-Virus (details see section 8.9 on page 127). After you have enabled this option, enter the required number of characters in the **Password** field and then retype the password in the **Confirm password** field.

8.7. Configuring prompts for confirmation

If you wish to be notified about certain events that happen during the program's operation, follow the Additional Settings link in the left part of the **Settings** tab (see Figure 6). Press the **Configure…** button in the **Confirmation prompts** section of the additional settings window that will open. As a result you will switch to the **Confirmation prompts settings** dialog box (see Figure 67).



☑ Prompt for the scan cancellation confirmation

☑ Prompt for confirmation when opening/closing the application

☑ Prompt for disabling real-time protection

☑ Prompt for processing dangerous objects

Figure 67. Configuring confirmation prompts

The following events are provided for:

☑ **Prompt for the scan cancellation confirmation** – display a prompt for the user to confirm an on-demand scan cancellation. When the scan is cancelled, a tooltip message will appear above the application icon in the system tray clarifying the reasons why the scan was cancelled.

☑ **Prompt for confirmation when opening/closing the application** – display a prompt to confirm opening/closing Kaspersky Anti-Virus Personal Pro.

☑ **Prompt for disabling real-time protection** – display warning messages to notify that the real-time protection of your computer was completely disabled. This box is not accessible if you disabled the use of the real-time file protection during the installation.

☑ **Prompt for processing dangerous objects** – display warnings stating that some infected objects remained unprocessed after the anti-virus scan.

8.8. Restricting the functionality of Kaspersky Anti-Virus

You can impose restrictions on launching Kaspersky Anti-Virus on demand scan in cases when you need to restrict the use of your computer's resources. In order to do it, follow the Additional settings hyperlink in the left part of the **Settings** tab (see Figure 6). In the additional settings configuration dialog box that will open switch to the **Efficiency** tab (see Figure 64).

You can impose the following restrictions:

☑ **Pause anti-virus scan when the system load exceeds ….%** - pause the on-demand anti-virus scan if the load on the file system exceeds the specified level. Once the file system load returns to the allowable level, the scan will be resumed. Specify the value for the allowable system load level using a slider or by entering this value in the field to the right of the slider (in percents) to pause the on-demand scan once this level is exceeded.

> This setting applies only to the on-demand scan tasks (for example a selected object scan task). Real-time anti-virus scan will not be interrupted.

☑ **Do not perform scheduled scan if the battery charge is below** – cancel the scheduled scan if you are using a portable computer and the battery charge is below a specified level. Specify the value for the allowable battery charge level using a slider or by entering this value in the field to the right of the slider (in percents) and the scheduled scan will be cancelled once the charge goes below this level.

> This option is available only if Kaspersky Anti-Virus is installed on a portable computer powered from a battery.

8.9. Working in the administrator’s and the user’s mode

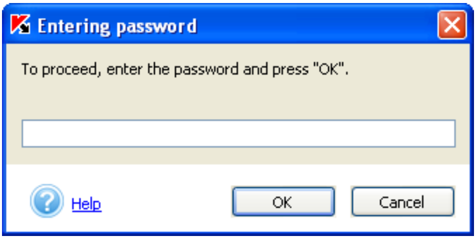
Kaspersky Anti-Virus can operate in two modes: the administrator’s and the user’s mode. The use of these modes can be useful if there is another user who has access to your computer. You can prohibit to this user to modify the anti-virus protection settings, disable the real-time protection and close Kaspersky Anti-Virus. In the user’s mode, the application interface changes, unavailable settings are no displayed (for example the main application window does not contain the **Settings** tab).

In order to enable the use of the user’s and the administrator’s mode:

Check the ☑ **Use password for application protection** box in the **Security** tab (see Figure 65) in the Kaspersky Anti-Virus **Additional settings** dialog box. Enter the required password in the **Password** field and retype it in the **Confirm password** field.

As the result, command **Switch to user mode** will appear in the application shortcut menu (see Figure 4) that you can use to switch to the user’s mode. In order to return to the administrator’s mode, use **Switch to administrator mode** command and enter the password in the window that will open (see Figure 68).

If the **Use password for application protection** box (see Figure 65) is not checked, Kaspersky Anti-Virus starts and operates in the administrator’s mode.



To proceed, enter the password and press "OK".

Figure 68. Entering password

CHAPTER 9. RENEWING YOUR LICENSE

You can use Kaspersky Anti-Virus Personal only after you have installed the license key included into the distribution kit.

⚠ Kaspersky Anti-Virus WILL NOT WORK without the license key!

After the license expires, Kaspersky Anti-Virus retains its functionality except for the anti-virus database and application module update services. You will still be able to scan your computer and email for viruses, and disinfect dangerous objects, but you will only be able to use out-of-date databases that were released on the date of the license expiration. Therefore, we do not guarantee 100% protection from new viruses that appear after your Kaspersky Anti-Virus license expires.

To avoid possible infection of your computer by new viruses, we recommend that you renew your Kaspersky Anti-Virus license.

Kaspersky Anti-Virus will notify you about the license expiration two weeks prior to the expiration date. A reminder message will be displayed each time you start the application during this period.

To renew your license, you must purchase and install a new license key for Kaspersky Anti-Virus Personal Pro. To obtain a new key:

1. Contact the vendor from whom you purchased the product and purchase a new Kaspersky Anti-Virus license key.

   or

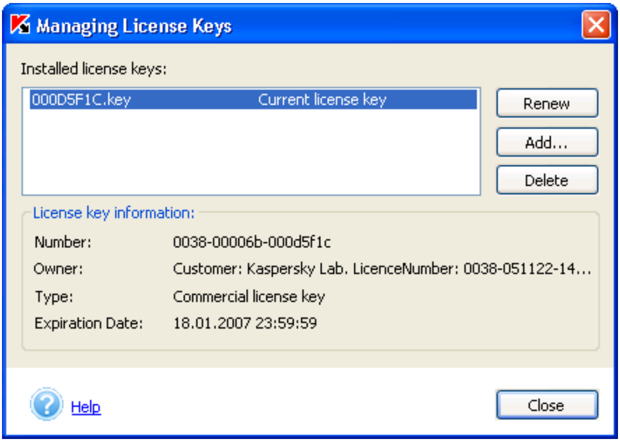
   Purchase a new license key directly from Kaspersky Lab by following the License Renewal link in the **Support** tab (see Figure 7) or by pressing the **Renew** button on the **Managing License Keys** window (see Figure 69) and filling out the corresponding form in the web page that will open. Upon receipt of your payment, we will send a link to the location where you can download the license key to the email address specified in your order form.

Kaspersky Lab on a regular basis offers an opportunity to renew license at low discounted prices. To enjoy these low prices, check section **Products→Renew your license** of our website on a regular basis.

2. Install the new license key as described below:

   a. Follow the License Keys in the left section of the **Support** tab (see Figure 7).

   b. In the **Managing License Keys** window (see Figure 69), press the **Add** button.



Installed license keys:

000D5F1C.key Current license key

License key information:

Number: 0038-00006b-000d5f1c

Owner: Customer: Kaspersky Lab. LicenceNumber: 0038-051122-14...

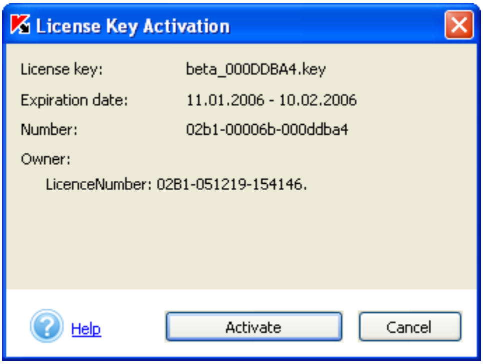
Type: Commercial license key

Expiration Date: 18.01.2007 23:59:59

Figure 69. The **Managing License Keys** window

   c. Using the standard file select dialog box, switch to folder containing the license key (file with extension **.key**). Select the required key and press the **Open** button.

   d. In the window that will open (see Figure 70), read about the license key you are adding and press the **Activate** button in order to activate this key.



License key: beta_000DDBA4.key

Expiration date: 11.01.2006 - 10.02.2006

Number: 02b1-00006b-000ddba4

Owner:

LicenceNumber: 02B1-051219-154146.

Figure 70. The **License Key Activation** dialog box

or:

a. Select the Kaspersky Anti-Virus Personal Pro group in the **Start→Programs** menu and select the **Install license key** item in the group menu.

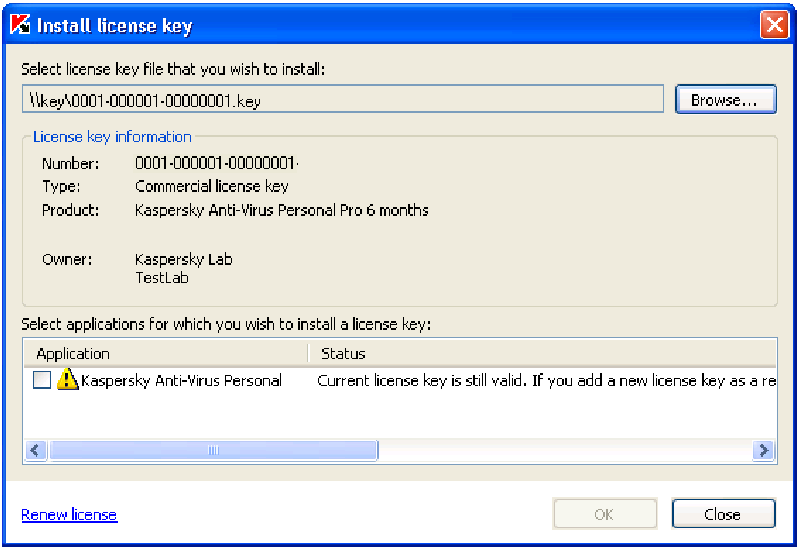
b. Press the **Browse** button in the window that will open and switch to the folder where the license key is located.

c. Select the required license file key and press the **Open** button.

d. In the bottom part of the bottom part of the window (see Figure 71) check the box next to the name of the application for which you wish to install the license key. Press the **OK** button.

If the list in the bottom part of the window is empty, the selected license key will not suit any of the Kaspersky Lab's applications installed on your computer.

Select a different license key file.



Install license key

Select license key file that you wish to install:

\\key\0001-000001-00000001.key

License key information

Number: 0001-000001-00000001-

Type: Commercial license key

Product: Kaspersky Anti-Virus Personal Pro 6 months

Owner: Kaspersky Lab
TestLab

Select applications for which you wish to install a license key:

Application	Status
□ Kaspersky Anti-Virus Personal	Current license key is still valid. If you add a new license key as a re

Figure 71. The **Install license key** dialog box

e. In the window that will open (see Figure 70), read about the license key you are adding and press the **Activate** button in order to activate this key.

CHAPTER 10. MANAGING APPLICATION FROM COMMAND LINE

Kaspersky Anti-Virus can be managed from the command line using the **kavshell.exe** utility included into the distribution kit of the product. After the installation of Kaspersky Anti-Virus, this utility will be located in the root installation folder of the application. When running the utility from the command line, the following functions are available depending on the keys used.

SCAN	scanning selected objects
FULLSCAN	full computer scan
UPDATE	updating the anti-virus database and application modules
ROLLBACK	rollback of the last update of the anti-virus database
RTP	managing the real-time protection mode of your computer
START	launching Kaspersky Anti-Virus
STOP	stopping Kaspersky Anti-Virus
TASK	managing Kaspersky Anti-Virus tasks
IMPORT	importing Kaspersky Anti-Virus settings from the file
EXPORT	exporting Kaspersky Anti-Virus settings to a file
ADDKEY	adding a license key

If you use your Kaspersky Anti-Virus with the option of switching between the user's and the administrator's mode disabled (see section 8.9 on page 127), commands that require password will not be performed. In this case an error message will be displayed.

In order to view the syntax of the command use:

```
KAVSHELL HELP [command] [6]
KAVSHELL [command] /?
```

If the **command** key is not supplied, the list of all available commands will be displayed.

For example:

```
KAVSHELL HELP SCAN
KAVSHELL SCAN /?
```

10.1. Scanning selected objects

Command syntax:

```
KAVSHELL SCAN [objects] [/L[!]:objects_file] [/F(A|E|C)]
[/NP] [/ASK|/DISINFECT|/DELETE] [/W[A][!]:report_file]
```

If no key is specified, the command syntax help will be displayed.

The scan task is performed with settings recommended by the Kaspersky Lab's experts.

objects	Defines a list of one or several files, folder or predefined objects separated by spaces. The following predefined objects can be used: • **/MEMORY** – system memory; • **/STARTUP** – startup objects; • **/MAIL** – Microsoft Office Outlook and Microsoft Outlook Express

[6] Optional keys are listed in the square brackets.

	mailboxes; • **/REMDRIVES** – removable drives; • **/FIXDRIVES** – system drives; • **/NETDRIVES** – network drives. Notes: • if the object name contains a space, such name shall be provided in quotes; • if you wish to scan several files you can use masks (examples of masks see 7.4 on page 97); • if a specific folder is indicated, all files contained in this folder will be scanned.
/L[!]:objects_file	Defines file in the **.txt** format containing the list of objects to be scanned (files, folders, predefined objects). The name of each object in the file must be entered on a new line. The **!** symbol is used to delete the file containing the list after the scan is completed. You can enter an absolute or relative path to the file. If the path contains a space, it must be entered in quotes.
/F(A|E|C) **/FA** **/FC** **/FE**	Types of files to be scanned: • scan all files. • scan infectable file based on the format. • scan infectable file based on the extension.
/NP	Skip password-protected objects
[/ASK|/DISINFECT|/DELETE] **/DISINFECT**	Action to be performed with the infected object: • Display prompt for processing a

/DELETE	detected infected object. • Disinfect, delete if disinfection is not possible. • Delete. Notes: • if no action is specified, the object will be skipped and information about its detection will be entered into the report; • composite files will not be deleted.
/W[A][!]:report_file **/W: report_file** **/WA: report_file**	Events output into the specified **report_file**: • only important events; • all events. The **!** symbol forces the report file to be re-written each time the task is started. A path to the file can be either absolute or relative. If the path contains a space, it must entered in quotes.

For example:

```
KAVSHELL SCAN "C:\Program Files" C:\Downloads\test.exe
/MEMORY /STARTUP /FA /DISINFECT /WA:log.txt
```

```
KAVSHELL SCAN /MEMORY /STARTUP C:\Downloads\test.exe /FC
/W:log.txt /ASK
```

10.2. Full scan

Command syntax:

```
KAVSHELL FULLSCAN [/W[A][!]:report_file] [/D]
```

If no key is specified, the command syntax help will be displayed.

The scan task is performed with settings recommended by the Kaspersky Lab's experts.

Key	**Purpose**
/W[A][!]:report_file **/W: report_file** **/WA: report_file**	Events output into the specified report_file: - only important events; - all events. The **!** symbol forces the report file to be re-written each time the task is started. A path to the file can be either absolute or relative. If the path contains a space, it must entered in quotes.
/D	Cancels the scan if this task has been already successfully performed today.

For example:

```
KAVSHELL FULLSCAN /WA:fullscan.log
```

10.3. Launching updates

Command syntax:

```
KAVSHELL UPDATE [updates_source]
[/W[A][!]:report_file] [/APP]
```

If no key is specified, the command syntax help will be displayed.

Key	**Purpose**
[updates_source]	An HTTP, FTP server or a network folder used to download updates. If the path is not specified, the updates source will be copied from the anti-virus database and application modules update task.

/W[A][!]: report_file **/W: report_file** **/WA: report_file**	Events output into the specified report_file: • only important events; • all events. The **!** symbol forces the report file to be re-writ ten each time the task is started. A path to the file can be either absolute or relative. If the path contains a space, it must entered in quotes.
/APP	Application modules updates.

For example:

```
KAVSHELL UPDATE ftp://ftp.kaspersky.ru/
/WA:avbases_upd.txt
KAVSHELL UPDATE /APP
```

10.4. Last update rollback

Command syntax

KAVSHELL ROLLBACK [/W[A][!]:report_file]

If no key is specified, the command syntax help will be displayed.

Key	**Purpose**
/W[A][!]: report_file **/W: report_file** **/WA: report_file**	Events output into the specified report_file: • only important events; • all events. The **!** symbol forces the report file to be re-written each time the task is started. A path to the file can be either absolute or relative. If the path contains a space, it must entered in quotes.

For example:

```
KAVSHELL ROLLBACK /WA:rollback.log
```

10.5. Real-time protection mode

Command syntax:

```
KAVSHELL RTP [taskid] { /START /PWD:password | /STOP
/PWD:password }
```

If no key is specified, the command syntax help will be displayed.

Key	**Purpose**
/START	Enables real-time protection or its specific component.
/STOP	Disables real-time protection or its specific component.
taskid	Real-time protection task's component identifier. If the identifier (tasked) is not specified, all commands will be applied to all real-time protection tasks. • on-access – real-time files protection; • mail-checker – real-time mail protection; • outlook-plugin – real-time Microsoft Office Outlook mail protection; • script-checker – real-time scripts monitoring; • office-guard – VBA-macros monitoring.
/PWD:password	Enter the administrator's password required for the execution of the command.

For example:

```
KAVSHELL RTP /START /PWD:password
KAVSHELL RTP on-access /START /PWD:password
KAVSHELL RTP /STOP script-checker /PWD:password
```

10.6. Starting application

Command syntax:

```
KAVSHELL START
```

10.7. Closing application

Command syntax:

```
KAVSHELL STOP /PWD:password
```

/PWD:password	Entering the administrator's password required to execute the command.

For example:

```
KAVSHELL STOP /PWD:password
```

10.8. Managing tasks

Command syntax::

```
KAVSHELL TASK [ taskid {/START  [/W[A][!]:report_file]|
                        /STOP |
                        /PAUSE |
                        /RESUME [/W[A][!][: report_file]]|
                        /DELETE } ] /PWD:password
```

If no key is specified, the list of all tasks with their unique identifiers will be displayed with the status for each task.

Key	Purpose
/START	Starts the task with the specified identifier.
/W[A][!]: report_file **/W: report_file** **/WA: report_file**	Events output into the specified report_file: • only important events; • all events. The **!** symbol forces the report file to be re-written each time the task is started. A path to the file can be either absolute or relative. If the path contains a space, it must entered in quotes.
/STOP	Stops the task with the specified identifier.

	Password is a mandatory parameter required to stop a real-time protection task: • real-time file protection • real-time mail protection • real-time scripts monitoring; • VBA macros monitoring; • protection against
/PAUSE	Pauses the execution of the task with the specified identifier.
/RESUME	Resumes the execution of the task with the specified identifier.
/DELETE	Deletes the task with the specified identifier.
taskid	Unique task identifier. You can manage the system tasks using the following standard identifiers: • scan-computer – full computer scan; • scan-removable – removable drives scan; • scan-quarantine – quarantine scan; • scan-critical – scan of disk boot sectors, memory, startup objects; • update-bases – anti-virus database updating; • update-app – application modules updating; • rollback – rollback of the last database update; • on-access – real-time files protection; • mail-checker - real-time mail protection; • script-checker – real-time scripts monitoring;

	- office-guard - VBA-macros monitoring; - ids - protection against network attacks.
/PWD:password	Enter the administrator's password required for the execution of the command.

For example:

```
KAVSHELL TASK /PWD:password
KAVSHELL TASK update-app /START /WA:fullscan.log
/PWD:password
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/DELETE /PWD:password
```

10.9. Importing/exporting settings

Command syntax:

```
KAVSHELL IMPORT settings_file /PWD:password
KAVSHELL EXPORT settings_file /PWD:password
```

Key	**Purpose**
settings_file	Name of the profile file from which Kaspersky Anti-Virus settings are exported or into which they are imported. Details on profiles see section 8.5 on page 119.
/PWD:password	Entering the administrator's password required to execute the command.

For example:

```
KAVSHELL IMPORT c:\kav50settings.xml /PWD:password
KAVSHELL EXPORT c:\kav50settings.xml /PWD:password
```

10.10. Adding a license key

Command syntax:

```
KAVSHELL ADDKEY file [/R] /PWD:password
```

Key	**Purpose**

`file`	License key file name
`[/R]`	Replacing the current license key with a new key.
`/PWD:password`	Entering the administrator's password required to execute the command.

For example:

```
KAVSHELL ADDKEY c:\00A531D2.key /R /PWD:password
```

CHAPTER 11. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to the most frequently asked questions from users pertaining to installation, setup and operation of the Kaspersky Anti-Virus; here we shall try to answer them here in detail.

***Question*: Is it possible to use Kaspersky Anti-Virus with anti-virus products of other vendors?**

We recommend uninstalling anti-virus products of other vendors prior to installation of Kaspersky Anti-Virus to avoid software conflicts.

***Question*: Kaspersky Anti-Virus does not rescan files that have been scanned earlier. Why?**

This is true. Kaspersky Anti-Virus does not rescan files that have not changed since the last scan.

That has become possible due to new iChecker and iStreams technologies. The technology is implemented in the program using a database of file checksums and file checksum storage in alternate NTFS streams.

***Question*: Why does Kaspersky Anti-Virus cause a certain decrease in server performance, noticeably loading the CPU?**

Virus detection is a computationally intensive mathematical problem requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by the anti-virus software, and each new virus added to the anti-virus database increases the overall scanning time. This is a necessary sacrifice for the security and safety of your data.

Other anti-virus products speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor, and file formats that require complicated analysis (e.g. PDF) from their databases. In contrast, Kaspersky Lab believes that the purpose of its anti-virus applications is to establish real and complete anti-virus security for its users. We believe that "partial protection" is even worse than no protection at all, because it forces users to take personal precautions.

Kaspersky Anti-Virus gives its users maximum protection. Experienced users can, of course, accelerate anti-virus scanning to the detriment of overall security by disabling scanning of various file types, but we do not recommend doing so for users who want the best protection.

For maximum user protection, Kaspersky Anti-Virus recognizes more than 700 formats of archived and compressed files. This is essential for anti-virus security, because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one. That is achieved through the use of new, exclusive technologies, such as iChecker™ and iStreams™, developed at Kaspersky Lab.

***Question**: Why do I need the license key file? Will my copy of the anti-virus application work without it?*

Kaspersky Anti-Virus does not work without a license key.

If you are still deciding whether or not to purchase Kaspersky Anti-Virus, you can download a trial version of the application from Kaspersky Lab's website **(Downloads → Trial Version)**. This trial version will only work for 15 days. When this period expires, the key will be blocked.

***Question**: What happens when the license expires?*

After expiration of the license, Kaspersky Anti-Virus will continue operating, but anti-virus database updating will be disabled. The anti-virus application will continue cleaning infected objects but only using the old anti-virus database.

If such a situation arises, contact for license extension the company from which you purchased your copy of Kaspersky Anti-Virus or directly Kaspersky Lab Ltd..

***Question**: What are the daily updates for?*

A few years ago viruses were transmitted on floppy disks, and adequate computer protection could be achieved by installation of an anti-virus program followed by rare updates to its anti-virus database. However, recent virus epidemics spread around the world in several hours, and anti-virus protection with old database may be helpless against a new threat. In order to resist new viruses, you should update the anti-virus database on a daily basis.

Each year Kaspersky Lab increases the frequency of its issued updates to the anti-virus database. Currently it is updated every hour.

Updating of the Anti-Virus application modules is an additional feature that allows both correction of discovered vulnerabilities and addition of new functions.

Question: What has changed in the updating service of version 5.0?

The Kaspersky Lab 5.0 product suite features a new updating service which has been developed in accordance with the requests of our users. It automates the whole updating procedure, from the preparation of updates in Kaspersky Lab to the moment that relevant files are updated on clients' computers.

Advantages of the new updating service include:

- *Ability to resume downloading of files after disconnection*. Upon reconnection only files which have not been downloaded are retrieved.
- Cumulative updates are now half the size. A cumulative update contains the whole anti-virus database, therefore its size exceeds considerably the size of typical updates. The new service employs a special technology which allows using already existing anti-virus database for a cumulative update.
- *Accelerated downloading from the Internet*. Kaspersky Anti-Virus picks up a Kaspersky Lab's updates server located in your region. Furthermore, servers are allocated according to their performance, so you will not be sent to an overloaded server while there is another idle server available.
- *Use of key “black lists“*. Unlicensed and illegal users are now prevented from using the updating service. Licensed users therefore do not suffer from inability to contact overloaded updates' servers.
- Corporate enterprises can now create a local updates' server. This feature is designed for organizations where a single LAN unites computers protected by Kaspersky Lab products. Any computer on the LAN can be turned into an updates' server that retrieves updates from the Internet and shares them with the other networked computers.

***Question*: Can an intruder replace my anti-virus database?**

All Kaspersky Lab anti-virus databases are supplied with a unique signature verified by Kaspersky Anti-Virus when the program is using them. If the signature supplied with the updated database does not match the signature assigned by Kaspersky Lab and if the database was released after your license for the product expired, Kaspersky Anti-Virus will not use such database.

***Question*: after the installation of Kaspersky Anti-Virus my connection to the local area network/internet was lost. What should I do?**

This means that you a firewall is installed on your computer. This resulted in a conflict with a network attacks protection module.

1. Open main application window of Kaspersky Anti-Virus Personal Pro and switch to the **Settings** tab (see Figure 6).
2. Using the Configure Real-Time Protection link, open the **Real-time protection settings** dialog box and choose the **Network** tab (see Figure 34).
3. Uncheck the **Enable real-time protection against network attacks** box and press the **OK** button.

In order to apply settings you have configured you have to restart your computer. In order to do this press the **Yes** button. If you wish to restart your computer later, press the **No** button.

***Question*: After the installation of Kaspersky Anti-Virus the operating system started "behaving" strangely ("blue screen of death", frequent restarting, etc.) What should I do?**

This means that there is a conflict between Kaspersky Anti-Virus and some software installed on your computer. In order to restore the functionality of your operating system do the following:

1. Press the **F8** key when the computer just started loading until the boot menu is displayed.
2. Select the **Safe Mode** item and load the operating system.
3. Open Kaspersky Anti-Virus.
4. Switch to the **Settings** tab in the main application window and press the Additional settings hyperlink.

5. Switch to the **Security** tab in the **Additional Settings** window that will open (see Figure 65) and uncheck the **Launch Kaspersky Anti-Virus at the system startup** box. Press the **OK** button.
6. Reload the operating system in the regular mode.

After this contact the Technical Support Service through the Kaspersky Lab’s corporate website (**Services→Technical Support)**. Describe in detail the problem and the circumstances in which this problem occurs.

Make sure that you attach to your question a file containing a complete dump of Microsoft Windows operating system. In order to create this file, do the following:

1. Right-click **My computer** and select the **Properties** item in the shortcut menu that will open.
2. Select the **Advanced** tab in the **System Properties** window and then press the **Settings** button in the **Startup and Recovery** section.
3. Select the **Complete memory dump** option from the drop-down list in the **Write debugging information** section of the **Startup and Recovery** window.

   By default, the dump file will be saved into the system folder as *memory.dmp*. You can change the dump storage folder by editing the folder name in the corresponding field.

4. Reproduce the problem related to the operation of Kaspersky Anti-Virus.
5. Make sure that the complete memory dump file was successfully saved.

Appendix A. Contacting Technical Support

Kaspersky Lab's Technical Support is available to all registered users of Kaspersky Anti-Virus in the following cases:

- If the application seems to work improperly and errors are frequently encountered.
- If Kaspersky Anti-Virus detects a suspicious file that contains critical data and the application denies access to it, while you need to continue working with the file.

If, while using Kaspersky Anti-Virus, you encountered problems, first of all you will have to check whether the method for solving your problem is described in the documentation, particularly, in section Frequently Asked Questions (see Chapter 11 on page 143) or in section **Services/Knowledge base** at the Kaspersky Lab's website (www.kaspersky.com).

If you have not found solution for your problem in the documentation and in the online Knowledge base, we recommend that you contact Kaspersky Lab's technical support service.

If you have a problem that must be solved immediately, follow the links specified in section C.2 on page 165. Phone support is provided 24/7 in Russian, English, French and German. Please pay attention that in order to obtain help, you must have a status of a registered user and provide your registration number (f you purchased a retail box version) or information on your order (if you purchased the product via the internet) to the Technical Support service representative.

To send a message to Kaspersky Lab's Technical Support about any failures encountered during application operation:

click Send question to technical support in the left section of the **Support** tab (see Figure 7) of the main application window.

This will automatically open Kaspersky Lab's website with the Technical Support request form. You have to fill out this form. In the first window of the form provide information about the problem and the Kaspersky Anti-Virus license details.

- Select the **Type of question** by selecting in the dropdown list the particular problem you have encountered while using Kaspersky Anti-Virus.
- Select **Kaspersky Anti-Virus Personal Pro** as the name of the Kaspersky Lab's product and provide a detailed description of the

problem you encounter in the **Detailed description of your question** field.

- Select the type of the application registration by indicating the **license key** if you purchased the product in the box and installed the license key from a disk or **online purchase** if you purchased the application online.
- Enter the serial number of the license in the **License serial number or online order** field. You can find this information in the **Number** field in the **Managing license keys** window (see Figure 69).
- Enter your e-mail address in the **Your e-mail address** field.
- Press the **Next** button.

In the next window of the form provide general information about the software, hardware and peripherals of your computer. You can enter this information manually using the corresponding fields of the form or use a special automatic information service. In order to do it make sure that your browser allows running ActiveX objects and press the **Fill-in** button. Additionally, provide the following information:

- If, while using Kaspersky Anti-Virus Personal Pro, you encountered a problem related to its compatibility with another application, please indicate the name of such application in the **Detected incompatibilities** field.
- Indicate your contact details in the **Contact information** section so that we can contact you in order to help you resolve this problem as soon as possible.
- Enter a special numeric code displayed in the Protection against automatic registration field to the left of the code and press the **Send question** button.

The application will automatically create a new message using the default mail client program installed in your computer, for example, Microsoft Office Outlook. It will automatically attach a text file to the message with a description of your system and all required data about your copy of Kaspersky Anti-Virus Personal Pro. You should provide a detailed description of the application fault that you encountered and send the message. Our technical consultants will respond to your request as soon as possible.

If Kaspersky Anti-Virus quarantines a file that is possibly infected, you may wish to update the anti-virus databases and try to disinfect the object (for details see section 8.2 on page 110). However, if this attempt to disinfect the file fails and you urgently need this file, please feel free to send the file to Kaspersky Lab for expert analysis. The file may be infected with an unknown virus or it may be a false alarm situation.

Attention! You may send files that you suspect to be infected to Kaspersky Lab only after you have scanned them using the database updated on the day you are sending the file.

To send a file to Kaspersky Lab for expert analysis:

select the file in the **Quarantine** window (see Figure 54) and click the Send button.

The application will automatically create and open a new message using the default mail client program installed in your computer, for example, Microsoft Outlook Express, with the suspicious file attached. Send this message. Kaspersky Lab will analyze the file you have sent and try to recover all data it contains. Whatever the outcome of the recovery, you will receive a detailed report with the results of the analysis.

Note that each of the files you send must have been scanned with Kaspersky Anti-Virus maximum one day before you send it.

It may happen that even though Kaspersky Anti-Virus does not detect any possibly infected files during the scan, you feel certain that one or more files in your computer are infected with a new virus. You can send such files to Kaspersky Lab for analysis.

To send files you suspect of being infected to Kaspersky Lab for expert analysis:

click Send file for analysis in the left section of the **Support** tab (see Figure 7). Select suspicious files using a standard Windows file selection dialog box.

The subsequent steps required to send a mail message to Kaspersky Lab are identical to the procedure of sending possibly infected objects from the **Quarantine** window.

Appendix B. Glossary

While reading this User's Guide you will encounter terms that have meanings specific to anti-virus protection. The intention of this Appendix is to provide an explanation of the meaning of such terms. The entries are listed in alphabetical order to simplify the search for the explanation you need.

A

Anti-virus database – A database created by Kaspersky Lab that contains a detailed description of all currently existing viruses and the methods used for their detection and disinfection. Our anti-virus database is regularly updated with information about new viruses as they appear; therefore, to keep your computer constantly protected from viruses, you need to *update* your anti-virus database as often as possible.

Anti-virus protection status – The current status of the anti-virus protection that characterizes the security level for your computer.

Archives – Files that include one or several files, which, in turn, can be archives.

B

Backing up – Creating a backup copy of a file in the BACKUP folder before treating it (disinfection or deleting). This file can later be restored from the backup copy, for example, for subsequent scanning with the current version of the anti-virus database.

BACKUP – The directory for saving backup copies of objects before their disinfection or deleting .

Boot sector – A special disk area that contains the operating system loader program.

Boot virus – A virus infecting *boot sectors* of computer disks. During a system boot, the virus forces the system to read it into memory and to surrender control from the original loader code to the viral code.

C

Computer memory – RAM installed in your computer.

D

Dangerous object – An object that contains a virus. We recommend that you refrain from using such objects in any way because this may lead to infection of your computer. If a dangerous object is found, we recommend that you try to *disinfect* it using Kaspersky Anti-Virus or *delete* it if disinfection is not possible.

Deleting an object – A method of treating an object. To delete an object means to remove it physically from your computer. This method is recommended for dangerous objects that for whatever reason cannot be disinfected.

Disk boot sector – An area on your hard drive or on any removable media (for example, a floppy disk or a CD-ROM). There are *boot viruses* that infect disk boot sectors*.* Kaspersky Anti-Virus scans boot sectors for viruses and *disinfects* them if infection is detected.

Disinfecting dangerous objects – A method of treating dangerous objects. Disinfection results in partial or full removal of malicious code from the infected data, or a decision that these files cannot be disinfected. Objects are disinfected using records contained in the *anti-virus database*.

E

Email databases – Special format databases that contain email messages stored on your computer. Every incoming/outgoing message is saved in the database after you receive/send it. These databases are scanned during a full scan of your computer. When real-time protection is enabled, Kaspersky Anti-Virus scans all incoming and outgoing email messages for viruses as they are being sent or received.

Exclusions – User-defined settings that exclude certain objects from the scan scope. You can customize exclusion rules for *real-time protection* and for *on-demand scans*. For instance, you can exclude archives from the scan scope during a full scan or, by using masks, specify certain file types that you do not want to scan.

F

False alarm – Situations when the application flags a clean object as infected because the code contained in this file resembles a viral code.

False positive – see *false alarm*

H

Heuristic code analyzer – A highly efficient technology that allows the application to detect unknown viruses. Objects that are suspected of being infected with either an unknown virus or a modified existing virus are identified using this technology.

High speed – A protection level that enables scanning of only *objects that may potentially become infected*. This significantly reduces scan time.

I

iChecker™ technology – a technology that allows to increase the speed of the anti-virus scan by excluding objects that have remain unchanged since the moment they had been last scanned, provided that the scan parameters (the anti-virus database and settings) have not changed. The relevant information used by the technology is stored in a special database.

For instance, you have an archived file that was scanned by Kaspersky Anti-Virus and assigned the "not infected" status. Next time this archive will be excluded from the scan scope if it has remained intact since then and the scan parameters have not 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.

The use of the iChecker™ technology is restricted to scanning only those objects that have structure known to Kaspersky Anti-virus (for example, exe, dll, lnk, tiff, inf, sys, com, chm, zip, rar).

iStreams™ technology – a technology similar to **iChecker™**. The difference between the two technologies is that when the iStreams™ technology is used, the information about the object scan results is stored in an additional file stream. Besides, the iStreams™ technology can be applied when scanning objects of any type irrespective of whether or not the structure of the object is known to Kaspersky Anti-Virus.

The iStreams™ technology is restricted to the use on NTFS file system disks only.

K

Kaspersky Anti-Virus Personal Pro application modules – Program library files included in the distributed copy of Kaspersky Anti-Virus Personal Pro. Each of these modules corresponds to a specific function of Kaspersky Anti-Virus, such as *real-time protection, on-demand scanning, updating.* When you start a full computer scan from the main application window, you initiate the launch of this task's module.

L

License key – A file with the *.key* extension that serves as your personal "key" required for the proper operation of Kaspersky Anti-Virus Personal Pro. The license key is included in the distribution kit if you purchase your copy of Kaspersky Anti-Virus from a Kaspersky Lab dealer. If you purchase the product online, the license key file will be sent to you via email. Kaspersky Anti-Virus WILL NOT WORK without the license key.

License period – A period during which you have the right to use Kaspersky Anti-Virus. The license period is defined by a valid license key and is, as a rule, one year from the date of purchase. After your license expires, the product will still work but you will not be able to update the *anti-virus database*.

M

Malware – the word is a contraction of "malicious software" and is a generic term for viruses, Trojans and worms.

Maximum protection – A protection level that ensures the maximum protection level that can be provided by Kaspersky Anti-Virus. With this protection mode, all files stored on your hard drive, removable media and network drives (if connected to your computer) are scanned for viruses.

O

OLE object – An object linked or embedded into another file. Kaspersky Anti-Virus scans such objects for viruses. For example, a Microsoft Excel spreadsheet embedded in a Microsoft Word document will be scanned by Kaspersky Anti-Virus as an OLE object.

On-demand scan – A mode of application operation initiated by the user that performs a scan of files of all types resident on your computer.

P

Packed files – Files containing a program and instructions for the program execution by the operating system.

Patch – A package of files used for updating programs. Patches are downloaded from the Internet and installed on your computer.

Possibly infected object – An object that contains code of an unknown virus or a code reminiscent of a known virus. Possibly infected objects are detected by the *heuristic code analyzer*.

Potentially infectable object – An object that has the potential to be infected. Potentially infectable objects are usually executable files, i.e. files with the *com*, *exe* and other extensions.

Prevention – A set of measures taken to prevent viruses from penetrating your computer. Computer virus prevention includes comprehensive anti-virus protection and retrieving current updates to your application.

Q

Quarantine – A folder to which Kaspersky Anti-Virus moves all *possibly infected objects* found during either a *full scan of your computer* or in *real-time protection* mode.

Quarantining (moving to the quarantine folder) – A method of treating a *possibly infected object* by denying normal access to the object and moving it to the quarantine folder for subsequent treatment.

R

Real-time protection – A mode of Kaspersky Anti-Virus operation when it is launched automatically at the system startup, in which all objects are scanned for viruses when they are accessed for reading, writing, or executing. If an object is identified as *dangerous* or *suspicious*, Kaspersky Anti-Virus will deny access to it and attempt to treat it (disinfect, quarantine, delete it, etc.) or prompt the user for action.

Recommended level – A level of anti-virus protection using settings recommended by Kaspersky Lab, which ensures the optimal protection of your computer. This level corresponds to the default settings.

Recovering, restoring – Moving an object from the *Quarantine/Backup storage* to its original folder, where it was located before it was quarantined/backed up, disinfected, or deleted; or moving an object to any other folder, specified by the user.

Report only – In this mode, when the application detects infected or suspicious objects it blocks access to them (in the real-time protection mode) and reports the detection in the task report log.

S

Scripts – A program file containing a sequence of actions which can, for example, be embedded into a web page and executed by the web browser (e.g. Microsoft Internet Explorer), or be standalone files for execution by the Windows operating system. In real-time protection mode, Kaspersky Anti-Virus monitors the execution of scripts, disables them, and scans for viruses. Depending on the results of the scan, you can, for example, allow or prohibit the script’s execution.

Skip – Method of treatment in which access to the object (only in real-time protection mode) will be denied, and information about the object will be recorded in the application operation report, but no other actions on the object will be performed.

Startup objects – A set of programs required for launching and correct operation of the operating system and other programs installed on your computer. Your operating system runs these objects during each startup. Some viruses infect startup objects and can prevent the operating system from loading.

Suspicious object – see *possibly infected object*.

T

Trusted processes – the list of software processes that are not monitored by Kaspersky Anti-Virus in the real-time protection mode. This means that all objects executed, opened or saved by the trusted process, will not be scanned.

U

Unknown virus – A new virus that is not registered in the *anti-virus database*. As a rule, Kaspersky Anti-Virus detects unknown viruses using the *heuristic code analyzer* and objects containing these viruses are flagged as *possibly infected*.

Updating the anti-virus database – A function of Kaspersky Anti-Virus that maintains the validity of the anti-virus protection of your computer. The updating process includes copying the *anti-virus database* from the Kaspersky Lab *update servers* to your computer and automatic integration of the database with Kaspersky Anti-Virus Personal Pro.

Update servers – A list of http- and ftp-servers updated regularly by Kaspersky Lab from which Kaspersky Anti-Virus copies the most recent version of the anti-virus database to your computer.

V

Virus attack – a series of actions intended to infect a computer with a virus or viruses.

Appendix C. Kaspersky Lab

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

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

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company’s products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company’s flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

C.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal has been designed to provide anti-virus protection to personal computers running Microsoft Windows 98/ME or Microsoft Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, Internet, floppy disks, CD, etc. The unique system of heuristic data analysis allows efficient neutralization of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scanning and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had already been scanned during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This feature **considerably increases the speed of the program's operation**.

The application creates a reliable barrier against viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocols and provides highly efficient detection of viruses in mail databases.

The application supports over 700 formats of archived and compressed files and provides automatic scanning of their content as well as removal of malicious code from **ZIP, CAB, RAR**, **ARJ**, **LHA** and **ICE** archives.

Configuring the application is made simple and intuitive due to the possibility to select one of three preset protection levels: **Maximum Protection**, **Recommended** or **High Speed**.

The anti-virus database is updated every hour and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the Internet or the connection has to be changed.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Microsoft Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, Kaspersky® Anti-Hacker blocks the suspicious application from accessing the network. This helps ensure enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite is a software suite designed for organizing comprehensive protection of personal computers running Microsoft Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection of data saved on your computer
- protection against spam for users of Microsoft Office Outlook and Microsoft Outlook Express
- protection of your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, for notifications about the current status of virus activity and fresh news. The program reads the list of available news channels and their content from news server of Kaspersky Lab with specified frequency.

The product performs the following functions:

- It visualizes in the system tray the current status of virus activity.
- The product allows the users to subscribe and unsubscribe from news channels.

- It retrieves news from each subscribed channel with the specified frequency and notifies about fresh news.
- It allows reviewing news on the subscribed channels.
- It allows reviewing the list of channels and their status.
- It allows opening pages with news details in your browser.

News Agent is a stand-alone Windows application, which can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

The program is a free service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus check of your computer. Kaspersky OnLine Scanner runs within your web browser using Microsoft ActiveX® technology. Thus, users can quickly test their computers in case of a slightest suspicion of malicious infection. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

Kaspersky® OnLine Scanner Pro

The program is a subscription service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your computer and disinfection of dangerous files. Kaspersky OnLine Scanner Pro runs within your web browser using Microsoft ActiveX® technology. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used as well as disinfection of e-mail databases.

- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, directories or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- **Control of changes within file system**. The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitoring of processes in random-access memory**. Kaspersky Anti-Virus 6.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in standard processes occur.
- **Monitoring of changes in OS registry** due to internal system registry control.
- **Blocking of dangerous VBA macros** in Microsoft Office documents.
- **System restoration** after malicious spyware influence accomplished due to recording of all changes in the registry and computer file system and an opportunity to perform their roll-back at user's discretion.

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 is an integrated solution for protection of personal computers against the main information-related threats, i.e. viruses, hackers, spam and spyware. A common user interface allows configuration and management of all solution components.

The anti-virus protection feature includes:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used. The program includes plug-ins for popular e-mail clients (Microsoft Office Outlook, Microsoft Outlook Express and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection**: anti-virus scanning of individual files, directories or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

- **Proactive protection**: the program performs constant monitoring of application activity and processes running in random-access memory preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is guaranteed owing to the ability to recognize phishing attacks, which helps prevent confidential data leaks (first of all, your passwords, bank account and credit card numbers), and block execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The feature **blocking charged phone calls** helps identify software that attempts to use your modem for hidden unauthorized connection to paid phone services and prevents such activity.

Kaspersky® Internet Security 6.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical hacker attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch into that mode, the system will block all network activity except for a few transactions allowed in user-defined rules.

The program employs complex approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites).

- Inspection of phrases in message body.

- Analysis of message text using a self-learning algorithm.

- Recognition of spam sent in image files.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of hand-held computers and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both in internal memory of PDA and smartphones or on memory cards of any type) on user demand;

- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a unique configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus protection[7] for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux.
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers.
- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a unique tool for automated deployment and administration.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;

[7] Depending on the type of distribution kit.

- *E-mail systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS, and also smartphones running Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam’s high performance is ensured by daily updates to the content filtration database adding samples provided by the Company’s linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for anti-virus processing of e-mail transmitted via SMTP. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a number of tools reducing the load on the mail system and preventing hacker attacks. DNS Black List support provides protection against e-mails coming from servers entered in these lists as sources distributing unwanted e-mail (spam).

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange performs anti-virus processing of incoming and outgoing mail messages as well as messages stored at the server, including letters in public folders and filters out unsolicited correspondence using "smart" spam recognition techniques in combination with Microsoft technologies.

The application scans all messages arriving at an Exchange Server via SMTP protocol checking them for the presence of viruses using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes. It filters out spam based on formal attributes (mail address, IP address, letter size, heading) and analyzes the content of messages and of their attachments using "smart' technologies, including unique graphic signatures for identifying graphic SPAM. The application scans both the message body and the attached files.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features.

C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

Appendix D. License Agreement

End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) PURCHASED ON LINE FROM THE KASPERSKY LAB INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF 7 WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation’s proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/ about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You

may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on ww.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means:

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential

information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Limitation of Liability.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii) below, you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).