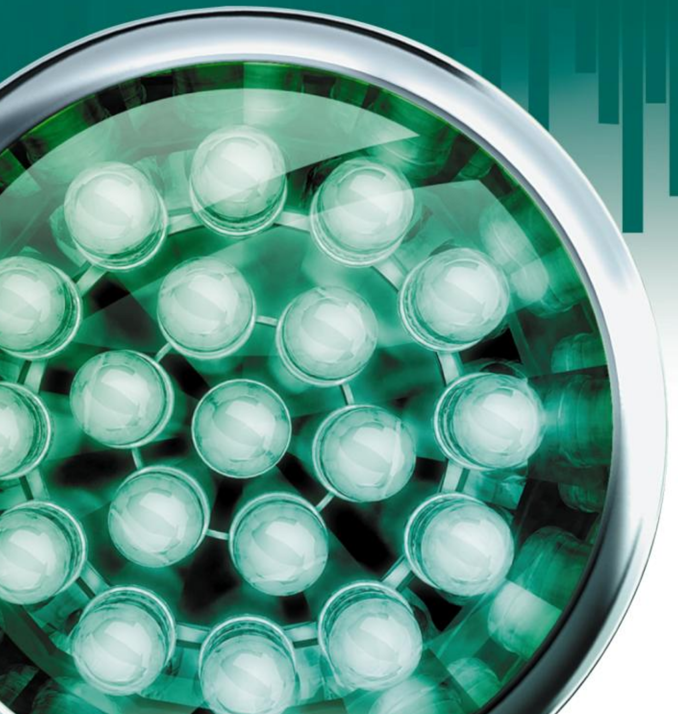
Kaspersky Anti-Virus 6.0 for Windows Workstations MP4

USER GUIDE

APPLICATION VERSION: 6.0 MAINTENANCE PACK 4, CRITICAL FIX 1



Dear User of Kaspersky Anti-Virus!

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

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

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

This document is subject to change without prior notification. For the latest version of this document please refer to Kaspersky Lab's website at http://www.kaspersky.com/docs.

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

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

Revision date: 25.02.2010

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

TABLE OF CONTENTS

INTRODUCTION

IN THIS SECTION

DISTRIBUTION KIT

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

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

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

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

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

END USER LICENSE AGREEMENT (EULA)

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

Read the EULA through carefully!

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

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

SERVICES PROVIDED FOR REGISTERED USERS

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

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

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

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

HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

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

General requirements:

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

Microsoft Windows 2000 Professional (Service Pack 4 Rollup1), Microsoft Windows XP Professional (Service Pack 2, or higher), Microsoft Windows XP Professional x64 (Service Pack 2, or higher):

- Intel Pentium 300 MHz 32-bit (x86) / 64-bit (x64) processor, or higher (or a compatible equivalent).
- 256 MB free RAM.

Microsoft Windows Vista Business / Enterprise / Ultimate (Service Pack 1, or higher), Microsoft Windows Vista Business / Enterprise / Ultimate x64 (Service Pack 1, or higher), Microsoft Windows 7 Professional / Enterprise / Ultimate, Microsoft Windows 7 Professional / Enterprise / Ultimate x64:

- Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) processor, or higher (or a compatible equivalent).
- 512 MB free RAM.

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS WORKSTATIONS MP4

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

What really sets Kaspersky Anti-Virus 6.0 for Windows Workstations apart from other software, even from other Kaspersky Lab's products, is the multifaceted approach to data security on the user's computer.

IN THIS SECTION

OBTAINING INFORMATION ABOUT THE APPLICATION

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

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

IN THIS SECTION

SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

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

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

Application page at the Kaspersky Lab website

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

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

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

http://support.kaspersky.com/wks

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

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

Help system

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

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

Documentation

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

CONTACTING THE SALES DEPARTMENT

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

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

The service languages are Russian and English.

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

CONTACTING THE TECHNICAL SUPPORT SERVICE

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

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

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

An email request to the Technical Support Service

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

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

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

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

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

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

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

Technical support by phone

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

DISCUSSING KASPERSKY LAB'S APPLICATIONS ON THE WEB FORUM

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

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

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

Kaspersky Anti-Virus 6.0 is a comprehensive data protection tool. The application ensures not only anti-virus protection but also protection against spam and network attacks. The application's components also enable users to protect their computers from unknown threats and phishing, and to restrict users' access to the Internet.

The multifaceted protection covers all channels for data transfer and exchange. Flexible configuration provided for any component lets users completely adapt Kaspersky Anti-Virus to their specific needs.

Let us take a closer look at the innovations in Kaspersky Anti-Virus 6.0.

New in protection:

- The new antivirus kernel that Kaspersky Anti-Virus uses detects malicious programs more effectively. The new antivirus kernel is also significantly faster in scanning the system for viruses. This is the result of improved object processing and optimized use of computer resources (particularly for dual or quad core processors).

- A new heuristic analyzer has been implemented, providing more accurate detection and blocking of previously unknown malicious programs. If a program's signature has not been found in anti-virus databases, the heuristic analyzer simulates the launch of the program in an isolated virtual environment. This method is secure and allows for analyzing all of the effects of a program before it runs in a real environment.
- The new Access Control component monitors users' access to external I/O devices, enabling administrators to restrict access to external USB drives, multimedia devices, and other data storage devices.
- Significant improvements have been made to the Firewall component (the overall effectiveness of the component has been improved and IPv6 support has been added) and Proactive Defense (the list of events processed by the component has been expanded).
- The update procedure for the application has been improved. The computer now rarely needs to be restarted.
- The ability to scan ICQ and MSN traffic has been added, which ensures the safe use of IM clients.

New interface features:

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

New features in Kaspersky Administration Kit:

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

WHAT KASPERSKY ANTI-VIRUS DEFENSE IS BUILT ON

Kaspersky Anti-Virus protection is built with the sources of threats in mind. In other words, each threat is dealt with by a separate application component that monitors it and takes the necessary actions to prevent malicious impact of that source on the user's data. This makes setup flexible, with easy configuration options for all components, which can be tailored to the needs of a specific user or the business as a whole.

Kaspersky Anti-Virus includes:

- Protection Components (on page 17) that provide defense that covers all channels of data transmission and exchange on your computer in real-time mode.
- Virus Scan Tasks (on page 18), with which the computer or separate files, folders, disks, or areas are scanned for viruses.

- Update (on page 18) that ensures the up-to-date status of the internal application modules and the databases used to detect malicious programs, network attacks, and spam messages.
- Support features (see section "Application support features" on page 18) provide information support for working with the application and expanding its capabilities.

PROTECTION COMPONENTS

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

File Anti-Virus (see page 43)

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

Mail Anti-Virus (see page 54)

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

Web Anti-Virus (see page 63)

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

Proactive Defense (see page 70)

Proactive Defense allows detecting a new malicious program before it performs its malicious activity. The component is designed around monitoring and analyzing the behavior of all applications installed on your computer. Judging by the actions executed by an application, Kaspersky Anti-Virus makes a decision if the application is potentially dangerous. So your computer is protected not only from known viruses, but from new ones as well that still have not been discovered.

Anti-Spy (see page 80)

Anti-Spy tracks the unauthorized advertising (banner ads, pop-up windows), intercepts the dialers attempting to establish a connection with pay-per-use websites, and block them.

Anti-Hacker (see page 84)

Anti-Hacker protects your computer while working on the Internet and other networks. It monitors inbound and outbound connections and scans ports and data packets.

Anti-Spam (see page 100)

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

Device Control (see page 118)

The component is designed to monitor the users' access to external devices installed on the computer. It limits the application's access to external devices (USB, Firewire, Bluetooth, etc.).

VIRUS SCAN TASKS

It is extremely important to scan your computer for viruses periodically. This is necessary in order to rule out the possibility of spreading malicious programs that have not been discovered by protection components because, for example, the security level had been set at low, or for other reasons.

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

Scan

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

Full Scan

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

Quick Scan

Virus scan of operating system startup objects.

UPDATE

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

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

SUPPORT FEATURES OF THE APPLICATION

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

Data files and reports

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

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

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

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

Rescue Disk

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

License

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

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

Support

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

Using the following links, you can access the Kaspersky Lab product users' forum, send an error report to Technical Support, or give application feedback by filling in a special online form.

You also have access to the online Technical Support and Personal User Cabinet Services. Our personnel are always happy to provide you with telephone support about Kaspersky Anti-Virus.

INSTALLING KASPERSKY ANTI-VIRUS 6.0

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

- local installation – application installation on a single computer. Direct access to that computer is required for the installation to run and complete. Local installation can be carried out in one of the following modes:
  - interactive mode, using the application installation wizard (see section "Installation using the Installation Wizard" on page 20); this mode requires the participation from the user when installing;
  - non-interactive mode in which the application installation is launched from the command line and does not require the participation from the user when installing (see section "Application installation from command line" on page 24).
- remote installation – application installation on networked computers managed remotely from an administrator's workstation using the following:
  - Kaspersky Administration Kit software set (see Kaspersky Administration Kit Deployment Guide);
  - group domain policies of Microsoft Windows Server 2000/2003 (see section "Installation from Group Policy Object editor" on page 24).

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

IN THIS SECTION

INSTALLATION USING THE INSTALLATION WIZARD

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

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

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

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

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

Step 1. Verifying that the system meets the installation requirements

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

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

Step 2. Installation start window

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

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

Step 3. Viewing the License Agreement

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

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

Step 4. Selecting installation folder

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

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

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

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

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

Step 5. Using application settings saved after previous installation

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

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

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

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

It is also recommended to use the Anti-Spam database if it has been saved after the previous version of the application had been removed. This will allow you to skip the procedure of Anti-Spam training. To consider the database you have created earlier, check the ☑ **Anti-Spam databases** box.

STEP 6. SELECTING THE TYPE OF THE INSTALLATION

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

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

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

To select the installation mode, click the corresponding button.

STEP 7. SELECTING APPLICATION COMPONENTS FOR THE INSTALLATION

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

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

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

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

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

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

STEP 8. DISABLING MICROSOFT WINDOWS FIREWALL

This step should be executed only if Kaspersky Anti-Virus is being installed on a computer where the firewall is enabled, and where Anti-Hacker is one of the components to be installed.

At this step of Kaspersky Anti-Virus installation, you will be offered to disable the Microsoft Windows firewall, since the Anti-Hacker component making part of Kaspersky Anti-Virus ensures complete protection for your network activity, and there is no need to build an additional protection within the operating system itself.

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

If you want to protect your computer with Microsoft Windows firewall, select the ● **Keep Windows Firewall enabled** option. In this case, the Anti-Hacker component will be installed but disabled to avoid conflicts in operation of applications.

STEP 9. SEARCHING FOR OTHER ANTI-VIRUS APPLICATIONS

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

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

You can choose whether to remove them automatically or manually, using the controls located below the list of detected anti-virus programs.

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

STEP 10. FINAL PREPARATION FOR INSTALLATION

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

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

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

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

When installing Kaspersky Anti-Virus components, which intercept network traffic, current network connections are terminated. The majority of terminated connections will be restored in due course.

STEP 11. COMPLETING THE INSTALLATION

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

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

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

APPLICATION INSTALLATION FROM THE COMMAND LINE

➡ *To install Kaspersky Anti-Virus 6.0 for Windows Workstations MP4, type the following in the command line:*

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

The installation wizard will run (see section "Installation using the Installation Wizard" on page 20). When the application is installed, the reboot is required.

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

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

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

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

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

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

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

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

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

When installing Kaspersky Anti-Virus in non-interactive mode, the setup.ini file reading is supported (see page 25); the file contains general settings for the installation of the application, *install.cfg* configuration file (see section "Import of protection settings" on page 197), and license key file. Note that those files should be located in the same folder as Kaspersky Anti-Virus installation package.

INSTALLATION FROM GROUP POLICY OBJECT EDITOR

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

INSTALLING THE APPLICATION

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

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

   Additionally, in this directory you can place the *setup.ini* file (see page 25), which contains the list of settings for Kaspersky Anti-Virus installation, the *install.cfg* configuration file (see section "Import of protection settings" on page 197), and a license key file.

2. Open **Group Policy Object editor** from the standard MMC console (for detailed information on how to work with this editor please refer to Microsoft Windows Server help system).

3. Create a new package. To do so, select **Group Policy Object / Computer configuration/ Program configuration / Software installation** from the console tree, and use the **Create / Package** command from the context menu.

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

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

DESCRIPTION OF SETUP.INI FILE SETTINGS

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

[Setup] – general settings for application installation.

- **InstallDir=**<path to application installation folder>.
- **Reboot=yes|no** – defines whether the computer should reboot when the application installation is complete, or not (reboot does not run by default).
- **SelfProtection=yes|no** – defines if Kaspersky Anti-Virus Self-Defense should be enabled during the installation (Self-Defense is enabled by default).
- **NoKLIM5=yes|no** – defines if the installation of Kaspersky Anti-Virus network drivers should be cancelled at the application installation (drivers are installed by default). Kaspersky Anti-Virus network drivers of NDIS type, which intercept the network traffic for such application components as Anti-Hacker, Mail Anti-Virus, Web Anti-Virus, and Anti-Spam, may cause conflicts with other applications or devices installed on the user's computer. You can skip the installation of network drivers on computers running under Microsoft Windows XP or Microsoft Windows 2000 to avoid probable conflicts.

This option in not available on computers running under Microsoft Windows XP x64 Edition or Microsoft Vista.

[Components] – selection of application components to be installed. If no component is specified, the application will be installed completely. If at least one component is specified, the components that have not been listed will not be installed.

- **FileMonitor=yes|no** – File Anti-Virus component installation.
- **MailMonitor=yes|no** – Mail Anti-Virus component installation.
- **WebMonitor=yes|no** – Web Anti-Virus component installation.
- **ProactiveDefence=yes|no** – Proactive Defense component installation.
- **AntiSpy=yes|no** – Anti-Spy component installation.
- **AntiHacker=yes|no** – Anti-Hacker component installation.
- **AntiSpam=yes|no** – Anti-Spam component installation.
- **LockControl=yes|no** – Device Control component installation.

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

- **ScanMyComputer=yes|no** – full scan task.
- **ScanStartup=yes|no** – quick scan task.
- **Scan=yes|no** – scan task.

- **Updater=yes|no** – update task for application databases and program modules.

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

UPDATING APPLICATION VERSION

➡ *To update Kaspersky Anti-Virus version, please do the following:*

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

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

REMOVING THE APPLICATION

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

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

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

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

GETTING STARTED

One of the main goals of Kaspersky Lab in creating Kaspersky Anti-Virus was to provide the optimum configuration of the application. This allows users with any level of computer literacy to ensure his or her computer's protection immediately after the installation without wasting his or her precious time upon the settings.

However, configuration details for your computer or for the tasks you execute with it can have their own specifics. That is why we recommend performing a preliminary configuration to achieve the most flexible, personalized approach to protecting your computer.

For the user's convenience, we have brought the preliminary configuration stages together in the unified interface of the Initial Configuration Wizard which starts upon the completion of the application installation procedure. Following the wizard's instructions, you will be able to activate the application, modify the update settings, restrict the access to the application using a password, and edit other settings.

Your computer can be infected with malware before the Kaspersky Anti-Virus is installed. To detect malware, run the computer scan (see section "Scanning computer for viruses" on page 120).

By the moment of the application installation, databases included in the installation package may become obsolete. Start the application update (on page 131) (unless it has been done using the setup wizard or automatically immediately after the application had been installed).

The Anti-Spam component included into the Kaspersky Anti-Virus package uses a self-training algorithm to detect unwanted messages. Run the Anti-Spam training wizard (see section "Training Anti-Spam using the Training Wizard" on page 103) to configure the component to work with your mail.

After completing the actions in this section, the application will be ready to protect your computer. To evaluate the level of your computer protection, use the Security Management Wizard (see section "Security management" on page 35).

IN THIS SECTION

INITIAL CONFIGURATION WIZARD

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

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

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

USING THE OBJECTS SAVED FROM THE PREVIOUS VERSION

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

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

ACTIVATING THE APPLICATION

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

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

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

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

- Online activation (see page 29). Select this activation option if you have purchased a commercial version of the application, and you have been provided an activation code. You can use this code to obtain a key file providing access to the application's full functionality throughout the effective term of the license.
- Activating trial version (see page 29). Use this activation option if you want to install the trial version of the application before making the decision to purchase a commercial version. You will be provided a free key file valid for a term specified in the trial version license agreement.
- Activation with a license key file obtained earlier (see section "Activating using a key file" on page 29). Activate the application using Kaspersky Anti-Virus 6.0 key file obtained earlier.
- Activate later. If you select this option, you will skip the activation stage. The application will be installed on your computer, and you will have access to all the application's features, except for updates (only one application update will be available, immediately after the installation). The **Activate later** option will only be available at the first startup of the Activation Wizard. At further wizard launches, if the application is already activated, the **Delete key file** option is available to perform the deletion.

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

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

You can also activate the application using Kaspersky Administration Kit. To do so, you should create a key file installation task (see page 212) (for more details please refer to the Kaspersky Administration Kit help guide).

SEE ALSO

ONLINE ACTIVATION

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

ENTERING THE ACTIVATION CODE

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

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

OBTAINING A KEY FILE

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

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

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

ACTIVATING THE TRIAL VERSION

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

ACTIVATION USING A KEY FILE

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

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

COMPLETING THE ACTIVATION

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

PROTECTION MODE

In this window, the Configuration Wizard asks you to select the protection mode in which the application will operate:

- **Basic protection**. This is the default mode that is designed for users who do not have extensive experience with computers or anti-virus software. It sets all the application's components to their recommended security levels and only informs the user of dangerous events, such as detecting malicious code or dangerous actions being executed.

- **Interactive protection**. This mode provides more customized defense of your computer's data compared to the Basic mode. It allows tracing the attempts of editing the system settings, suspicious system activity, and unauthorized operations on the network.

  Each of these actions may either be provoked by the activity of a malicious program, or be standard feature for the functioning of the applications installed on your computer. You will have to decide for each separate case whether those activities should be allowed or blocked.

  If you select this mode, specify when it should be used:

  - ☑ **Enable Anti-Hacker Training Mode** prompts user to accept actions when programs installed on your computer try to connect to a network resource. You can either allow or block that connection and configure Anti-Hacker rules for that application. If you disable Training Mode, Kaspersky Anti-Virus runs with minimal protection settings, meaning that it grants all applications access to network resources.

  - ☑ **Enable Registry Guard** prompts user for a response when attempts of modifying system registry objects are detected.

UPDATE SETTINGS CONFIGURATION

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

- ◉ **Automatically**. Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scanning frequency may increase during anti-virus outbreaks and decrease when they are over. If new updates are found, Kaspersky Anti-Virus downloads and installs them on the computer. This is the default mode.

- ◉ **Every 2 hour(s)** (frequency may vary depending on the schedule settings). Updates will run automatically according to the schedule created. You can modify the schedule settings in another window by clicking the **Change** button.

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

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

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

CONFIGURING VIRUS SCAN SCHEDULE

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

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

Full Scan

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

Quick Scan

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

RESTRICTING ACCESS TO THE APPLICATION

Since a personal computer may be used by several people with different levels of computer literacy, and since malicious programs can disable its protection, you have the option of password-protecting access to Kaspersky Anti-Virus. Using a password can protect the application from unauthorized attempts to disable protection, change the settings, or uninstall the application.

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

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

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

CONFIGURING ANTI-HACKER

Anti-Hacker is the component of Kaspersky Anti-Virus that secures your computer on local networks and on the Internet. At this stage, the Configuration Wizard offers you to create a list of rules that would guide Anti-Hacker when analyzing your computer's network activity.

SEE ALSO

DETERMINING A SECURITY ZONE’S STATUS

In this stage, the Configuration Wizard analyzes your computer’s network environment. Based on the analysis, the entire network space is broken down into conventional zones:

- *Internet* – the World Wide Web. In this zone, Kaspersky Anti-Virus operates as a personal firewall. At that, default rules for packets and applications regulate all network activity to ensure maximum security. You cannot change protection settings when working in this zone, unless enable Stealth Mode on your computer for added safety.

- *Security zones* – certain conventional zones that mostly correspond with subnetworks that your computer is added in (these could be local subnetworks at home or in office). By default, these zones are considered as average-risk zones when working in them. You can change the statuses of these zones based on how much you trust a certain subnetwork, and you can configure rules for packet filtering and applications.

All detected zones will be displayed on a list. Each of them is shown with a description, address and subnetwork mask. The list also contains statuses according to which any given network activity will be allowed or blocked within the scope of Anti-Hacker component operation:

- **Internet**. This is the default status assigned to the Internet, since when you are on it, your computer is subjected to all types of potential threats. It is recommended to select this status for networks not protected by any anti-virus applications, firewalls, filters etc. When you select this status, the application ensures maximum security for this zone:

  - blocking any network NetBIOS activity within the subnetwork;

  - blocking rules for applications and packet filtering that allow NetBIOS activity within this subnetwork.

  Even if you have created a shared folder, the information in it will not be available to users from subnetwork with this status. Additionally, if this status is selected for a certain subnetwork, you will not be able to access files and printers on other computers of this subnetwork.

- **Local network**. The application assigns this status to the majority of security zones detected when analyzing the computer’s network environment, except for the Internet. This status is recommended for zones with an average risk factor (for example, corporate LANs). If you select this status, the application allows the following:

  - any network NetBIOS activity within the subnetwork;

  - applying rules for applications and packet filtering that allow NetBIOS activity within this subnetwork.

  Select this status if you want to grant access to certain folders or printers on your computer but block any other external activity.

- **Trusted**. It is only recommended to apply this status to zones that in your opinion are absolutely safe where your computer is not subject to attacks and attempts to gain access to your data. If you select this status, all network activity will be allowed. Even if Maximum Protection is selected and block rules are created, they will not function for remote computers from a trusted zone.

You can use *Stealth Mode* for added security when using networks labeled **Internet**. This feature only allows network activity initiated from your computer. This actually means that your computer becomes invisible to its surroundings. This mode does not affect your computer’s performance on the Internet.

It is not recommended to use the Stealth Mode if the computer is being used as a server (for example, mail server or HTTP server). Otherwise, the computers that connect to the server will not see it in the network.

To change the status of a zone or to enable/disable Stealth Mode, select it from the list, and use the corresponding links in the **Rule description** box below the list. You can perform similar actions as well as edit addresses and subnetwork masks in the **Zone settings** window which you can open with the **Edit** button.

You can add a new zone to the list while viewing it. To do so, click the **Refresh** button. Anti-Hacker will search for available zones for registration, and if any are detected, the program will ask you to select a status for them. Besides, you can add new zones to the list manually (for example, if you connect your laptop to a new network). To do so, use the **Add** button and enter required information in the **Zone settings** window.

To delete the network from the list, click the **Delete** button.

CREATING THE LIST OF NETWORK APPLICATIONS

The Configuration Wizard analyzes the software installed on your computer and creates a list of applications that use a network connection.

Anti-Hacker creates a rule to control network activity of each application like these. The rules apply using templates for the most common applications that use network connections, created at Kaspersky Lab and included with the product.

You can view the list of network applications and the rules for them in the Anti-Hacker settings window that you can open by clicking the **Applications** button.

For added security, we recommend disabling DNS caching when browsing Internet resources. This feature dramatically decreases the time your computer spends to connect to a required Internet resource; however, it is at the same time a dangerous vulnerability, and by using it, intruders can provoke data leakages that cannot be traced using the firewall. Therefore, to increase the degree of security for your computer, we recommend disabling the option of saving information about domain names in the cache.

FINISHING THE CONFIGURATION WIZARD

The Wizard's last window will ask if you want to restart your computer to complete the application installation. You should restart for Kaspersky Anti-Virus drivers to register.

You can delay the restart, but the application will not be fully functional until after the restart.

SCANNING COMPUTER FOR VIRUSES

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

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

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

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

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

UPDATING THE APPLICATION

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

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

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

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

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

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

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

MANAGING LICENSES

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

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

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

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

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

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

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

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

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

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

1. Purchase a new key file or an activation code. Use the **Purchase license** (if the application has not been activated) or **License renewal** button. On the web page that will open you will be provided with detailed information on the terms of purchasing the key from Kaspersky Lab eStore or from authorized distributors. If you purchase online, a key file or an activation code will be mailed to you at the address specified in the order form once payment has been made.

2. Activate the application. Use the **Add / Delete** button in the **License** section of the main application window, or use the **Activate** command from the application context menu. This will start the Activation Wizard.

SECURITY MANAGEMENT

Problems in computer protection are indicated by the computer protection status (see section "Main application window" on page 40), which is displayed by changes in color of the protection status icon and of the panel on which it is located. Once problems appear in the protection, you are advised to solve them.

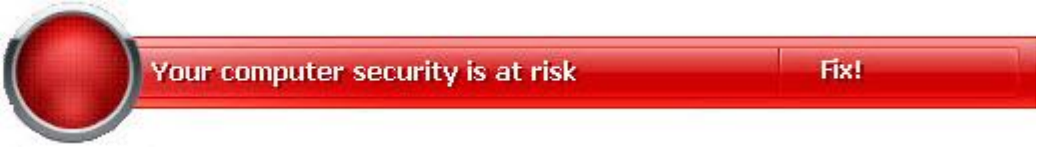
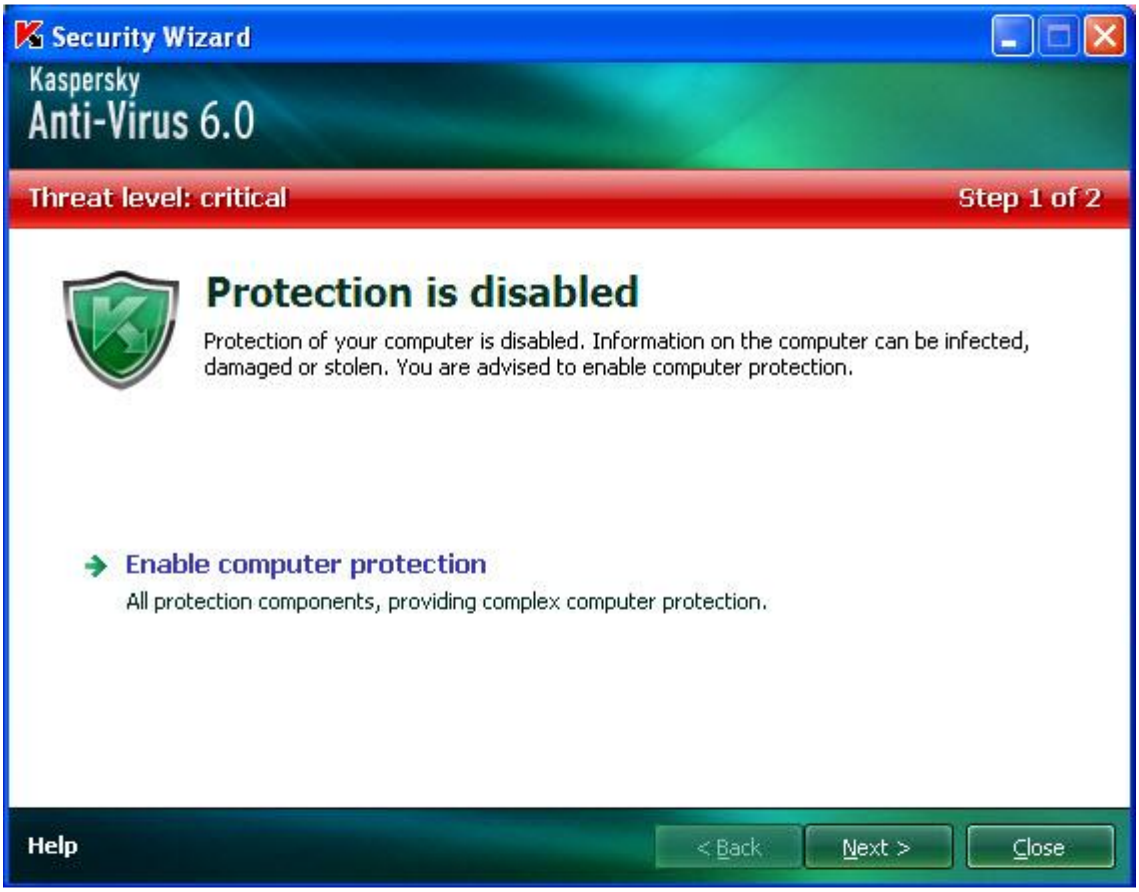


Figure 1. Current status of the computer protection

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



Threat level: critical

Step 1 of 2

Protection is disabled

Protection of your computer is disabled. Information on the computer can be infected, damaged or stolen. You are advised to enable computer protection.

Enable computer protection

All protection components, providing complex computer protection.

Figure 2. Solving security problems

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

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

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

PAUSING PROTECTION

Pausing protection means temporarily disabling all the protection components that monitor the files on your computer, incoming and outgoing mail, Internet traffic, applications' behavior, Anti-Hacker, and Anti-Spam.

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

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

ELIMINATING PROBLEMS. USER TECHNICAL SUPPORT

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

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

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

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

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

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

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

CREATING A TRACE FILE

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

➡ *To create the trace file:*

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

CONFIGURING APPLICATION SETTINGS

The application settings window (see page 142) that can be accessed from the main window by clicking the **Settings** button, is designed for the quick access to Kaspersky Anti-Virus 6.0 settings.

APPLICATION OPERATION REPORTS. DATA FILES

The operation of each Kaspersky Anti-Virus component and the performance of each virus scan and update task are recorded in a report (see page 163). To view reports, use the **Reports** button in the lower right corner of the main window.

The objects that have been quarantined (see page 164) or placed to the backup (see page 165) by Kaspersky Anti-Virus, are called *application data files*. By pressing the **Detected** button, you can open the **Storage** window, where you can process these objects as necessary.

APPLICATION INTERFACE

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

In addition to the basic interface, the application has expansion components (plugins) integrated into Microsoft Office Outlook (scan for viruses and scan for spam), Microsoft Outlook Express (Windows Mail), The Bat! (scan for viruses and scan for spam), Microsoft Internet Explorer, and Microsoft Windows Explorer applications. The plugins expand the features of these programs by making Kaspersky Anti-Virus management and settings possible from their interfaces.

In this section

See also

TASKBAR NOTIFICATION AREA ICON

Immediately after installing Kaspersky Anti-Virus, the application icon will appear in the Microsoft Windows taskbar notification area.

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

If the icon is active (in color), it means that protection is enabled on your computer. If the icon is inactive (grey), it means that all protection components (on page 17) are disabled.

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

- – email being scanned.
- – HTTP traffic scan in progress.
- – a file that you or some program are opening, saving, or running is being scanned.
- – Kaspersky Anti-Virus database and module update is in progress.
- – computer should be rebooted to apply updates.
- – an error has occurred in the operation of some Kaspersky Anti-Virus component.

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

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

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

CONTEXT MENU

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

- **Full Scan –** start a complete scan (see page 120) of your computer for malicious objects. Objects residing on all drives, including removable storage media, will be scanned.
- **Scan –** select objects and start the scan for viruses. By default, the list contains a number of files, such as the **My Documents** folder, Startup objects, email databases, all disk drives on your computer, etc. You can enlarge the list, select other objects for scan and start virus scan.
- **Update** – starts updates (see page 131) for application modules and databases of Kaspersky Anti-Virus and installs them on your computer.
- **Network Monitor** – view the list (see page 96) of network connections established, opened ports, and traffic.
- **Activate** – activates the application (see page 28). To become a registered user with access to the application's full functionality and Technical Support, you have to activate your version of Kaspersky Anti-Virus. This menu item is only available if the application has not been activated.
- **Settings** – view and edit settings (see page 142) of Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus** – open the main application window (see page 40).
- **Pause Protection / Resume Protection** – temporarily disable or enable protection components (see page 17). This menu option does not affect the application’s updates, or the execution of virus scans.
- **Disable policy / Enable policy –** temporarily disable or enable policy when application is working via Kaspersky Administration Kit. This menu item allows removing the computer from the scope of policies and group tasks. This opportunity is managed with a password. The menu item only appears if a password is set.
- **About** – display the window with information about the application.
- **Exit** – close Kaspersky Anti-Virus (when this option is selected, the application will be discarded from the computer’s RAM).

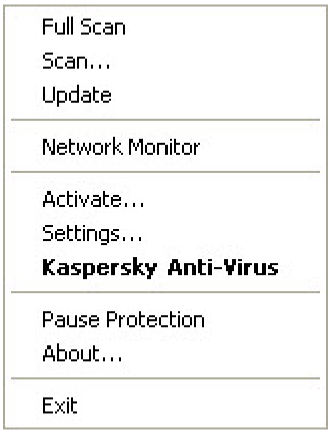


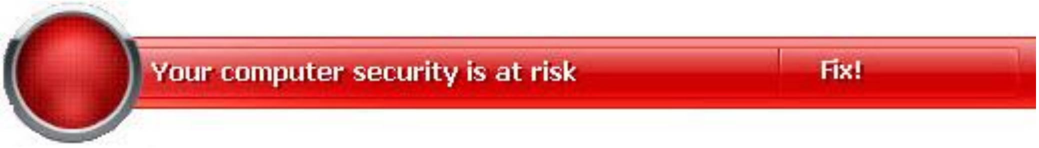
Figure 3. Context menu

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

MAIN APPLICATION WINDOW

The main application window can be divided into three parts:

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



Your computer security is at risk

Fix!

Figure 4. Current status of the computer protection

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

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

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

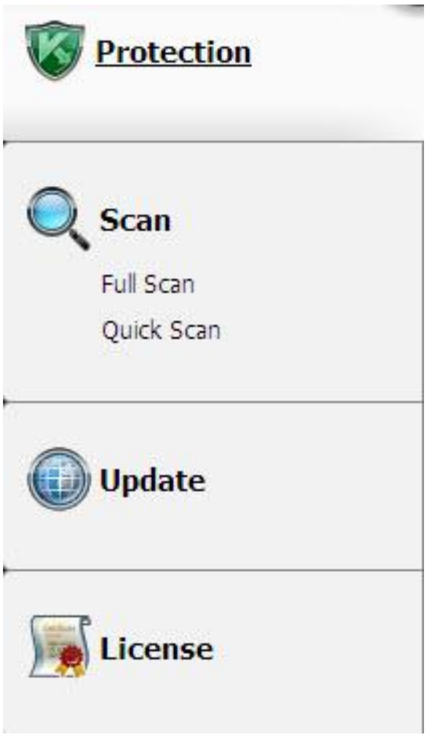
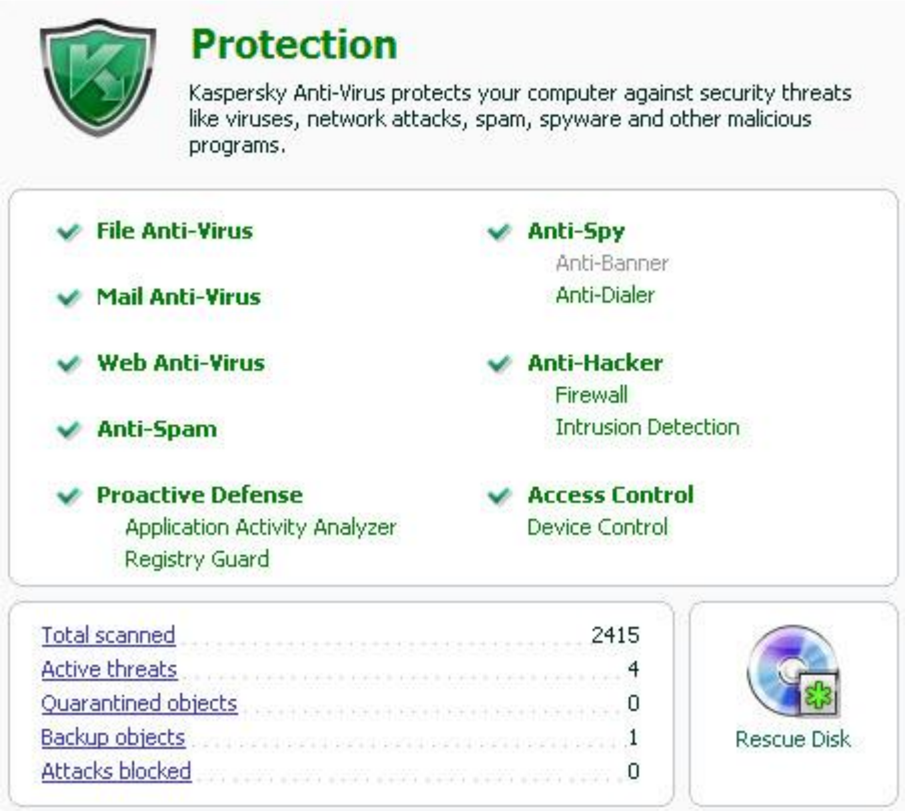


Figure 5. Left part of the main window

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



Protection

Kaspersky Anti-Virus protects your computer against security threats like viruses, network attacks, spam, spyware and other malicious programs.

✓ File Anti-Virus

✓ Mail Anti-Virus

✓ Web Anti-Virus

✓ Anti-Spam

✓ Proactive Defense
Application Activity Analyzer
Registry Guard

✓ Anti-Spy
Anti-Banner
Anti-Dialer

✓ Anti-Hacker
Firewall
Intrusion Detection

✓ Access Control
Device Control

Total scanned	2415
Active threats	4
Quarantined objects	0
Backup objects	1
Attacks blocked	0

Figure 6. Right part of the main window

You can also use:

- The **Settings** button – to open the application settings window (see page 142);
- The **Help** link – to open Kaspersky Anti-Virus Help;
- The **Detected** button – to work with application datafiles (see page 162);
- The **Reports** button – to open the reports of the components (see page 163) of the application;
- The **Support** link – to open the windows containing the information about the system and the links to Kaspersky Lab's information resources (see page 36) (Technical Support service site, forum).

NOTIFICATIONS

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

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

- **Alarm**. A critical event has occurred; for instance, a virus or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. This type of notification is color-coded in red.
- **Warning**. A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide how dangerous you think this event is. This type of notification is color-coded in yellow.

- **Info**. This notification gives information about non-critical events. This type, for example, includes notifications related to the operation of the Anti-Hacker component. Minor notifications are color-coded in green.

SEE ALSO

APPLICATION SETTINGS WINDOW

Kaspersky Anti-Virus settings window may be opened via the main window or the context menu. To do so, click the **Settings** button in the top part of the main window, or select the appropriate option in the application's context menu.

The application settings window consists of two parts:

- the left part of the window provides access to Kaspersky Anti-Virus components, virus scan tasks, update tasks, etc.;

- the right part of the window contains a list of settings for the component, task, etc., selected in the left part of the window.

SEE ALSO

FILE ANTI-VIRUS

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

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

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

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

➧ *To modify File Anti-Virus settings:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

COMPONENT OPERATION ALGORITHM

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

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

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

The scan includes the following steps:

- The file is scanned for viruses. Objects are detected by comparing them with the application databases. The database contains descriptions of all malicious programs and threats currently known, and methods for processing them.
- After the analysis you have the following available courses of action for Kaspersky Anti-Virus:

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

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

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

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

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

SEE ALSO

File Anti-Virus 43

CHANGING SECURITY LEVEL

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

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

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

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. Select the required security level in the window that will open.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

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

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

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

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

All possible actions are shown in the table below.

IF THE ACTION SELECTED WAS	WHEN A DANGEROUS OBJECT IS DETECTED
● **Prompt for action**	File Anti-Virus displays a warning message containing information about what malicious program has infected or potentially infected the file and gives you a choice of action. Depending on the status of the object, actions may vary.
● **Block access**	File Anti-Virus blocks access to the object. Relevant information is logged in the report. Later you can attempt to disinfect this object.
● **Block access** ☑ **Disinfect**	File Anti-Virus blocks access to the object and attempts to disinfect it. If it is successfully disinfected, it is restored for regular use. If the attempt of disinfecting the object fails, it will be either blocked (if the object cannot be disinfected), or assigned the *potentially infected* status (if the object is considered suspicious), and it will be moved to Quarantine. Relevant information is logged in the report. Later you can attempt to disinfect this object.
● **Block access** ☑ **Disinfect** ☑ **Delete if disinfection fails**	File Anti-Virus blocks access to the object and attempts to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be disinfected, it is deleted. A copy of the object will be stored in Backup.
● **Block access** □ **Disinfect** ☑ **Delete**	File Anti-Virus blocks access to the object and deletes it.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it, which is placed into Backup to allow later restoration or disinfection.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. Select the required action in the window that will open.

CREATING A PROTECTION SCOPE

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

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

When selecting file types you should remember the following:

- There are a number of file formats that have a fairly low risk of having malicious code infiltrated into them and subsequently activated (for example, *.txt*). Conversely, there are formats that contain or can contain executable code, for instance *.exe*, *.dll*, *.doc*. The risk of activating malicious code in such files is quite high.

- Remember that an intruder can send a virus to your computer in a file with the *.txt* extension, whereas it is in fact an executable file renamed as *.txt* file. If you have selected the **Files scanned by extension** option, such a file would be skipped by the scan. If the **Files scanned by format** setting has been selected, then, regardless of the extension, File Anti-Virus will analyze the file header, uncover that the file is an *.exe* file, and scan it for viruses.

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

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

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

➧ *To edit the object scan list:*

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

➧ *To change the type of scanned objects:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **General** tab, in the **File types** section, select required settings.

USING HEURISTIC ANALYSIS

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

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

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Performance** tab, in the **Scan methods** section, check the ☑ **Heuristic analysis** box and specify the detail level for the scan.

SCAN OPTIMIZATION

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Performance** tab, check the ☑ **Scan new and changed files only** box.

SCAN OF COMPOUND FILES

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

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

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

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, check the boxes for the types of compound files to be scanned.

SCANNING LARGE COMPOUND FILES

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

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Performance** tab, in the **Scan of compound files** section, click the **Additional** button.
6. In the **Compound files** window, check the ☑ **Extract compound files in the background** box and specify the minimum file size value in the field below.

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

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

CHANGING THE SCAN MODE

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

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

➧ *To change the object scan mode:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Additional** tab, in the **Scan mode** section, select the required mode.

SCAN TECHNOLOGY

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

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

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

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

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

➧ *To change the object scan technology:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Additional** tab, in the **Scan technologies** section, select the required setting value.

PAUSING THE COMPONENT: CREATING A SCHEDULE

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

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

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

PAUSING THE COMPONENT: CREATING A LIST OF APPLICATIONS

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

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

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

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

RESTORING DEFAULT PROTECTION SETTINGS

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

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **File Anti-Virus** component context menu, select the **Settings** item.
4. In the window that will open, click the **Default level** button.
5. In the **Restore settings** window that will open, check the ☑ **Protection scope** box.

FILE ANTI-VIRUS STATISTICS

All operations performed by File Anti-Virus are recorded in a special report where you can obtain detailed information on the component's operation grouped on tabs:

- All dangerous objects detected during the file system protection process are listed on the *Detected* tab. Here you will find the full path to the location of each object and the status assigned to it by File Anti-Virus. If the component has successfully established what malicious program had infected the object, the latter will be assigned the appropriate status: for example, *virus*, *Trojan*, etc. If the type of malicious impact cannot be exactly established, the object is assigned the *suspicious* status. The action applied to the object (detected, not found, disinfected) is also shown next to the status.
- The complete list of events that have occurred while using File Anti-Virus is kept on the *Events* tab. Events may have the following statuses:
  - *information* (for example, object not processed, skipped by type);
  - *warning* (for example, a virus is detected);
  - *comment* (for example, archive is password-protected).

  As a rule, informative messages are reference-type messages and are not of particular interest. You can disable display of informative messages. To do so, uncheck the ☑ **Show all events** box.
- Scan *statistics* appear on the appropriate tab. Here you will find the total number of objects scanned, and then special columns separately display how many objects out of the total number scanned are archives, how many of them are dangerous, how many have been disinfected, how many have been quarantined, etc.
- The settings that File Anti-Virus is running with are displayed on the *Settings* tab. Use the **Change settings** link to quickly configure the component.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **File Anti-Virus** component context menu.

DELAYED OBJECT TREATMENT

If you have selected ● **Block access** as the action for malicious objects, they will not be disinfected and access to them will be blocked.

If the actions selected were:

◉ **Block access**

☑ **Disinfect**

all non-disinfected objects will also be blocked.

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

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

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

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

MAIL ANTI-VIRUS

Mail Anti-Virus scans incoming and outgoing messages for the presence of malicious objects. It is launched when the operating system loads, is located in the RAM and scans all email messages being transmitted via the POP3, SMTP, IMAP, MAPI, and NNTP protocols. Also, the component scans traffic of ICQ and MSN instant messaging clients.

A collection of settings called the security level, determines the way of scanning the email. If Mail Anti-Virus detects a threat, it will perform the specified action. The rules with which your email is scanned are defined by a collection of settings. The settings can be broken down into the following groups:

- settings that determine the protected stream of messages;
- settings that determine the use of heuristic analysis methods;
- settings that determine the scan of compound files;
- settings that determine the filtering of attached files.

Kaspersky Lab advises abstaining from configuring Mail Anti-Virus on your own. In most cases, selecting a different security level is sufficient.

If Mail Anti-Virus has been disabled for any reason, connections to the mail server established before it had been enabled, will not be monitored. Also, the traffic of IM clients will not be monitored if traffic scan has been disabled (see page 57). The application should be restarted immediately after traffic scan is enabled, or after Mail Anti-Virus is run.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

COMPONENT OPERATION ALGORITHM

Mail Anti-Virus loads when the operating system launches and runs continually, scanning all email on the POP3, SMTP, IMAP, MAPI and NNTP protocols, as well as on secure connections (SSL) for POP3 and IMAP.

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

By default, email protection is carried out as follows:

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

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

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

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

   - If the body or attachments of the email contain malicious code, Mail Anti-Virus will block the email, place a copy of the infected object in the *backup*, and try to disinfect the object. If the email is successfully disinfected, it becomes available to the user again. If the disinfection fails, the infected object in the email is deleted. After the virus scan, special text is inserted in the subject line of the email, stating that the email has been processed by the application.

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

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

An integrated extension module is provided for Microsoft Office Outlook (see section "Email scanning in Microsoft Office Outlook" on page 59) that allows fine-tuning the email scan.

If you are using The Bat!, the application can be used in conjunction with other anti-virus applications. The email traffic processing rules (see section "Email scanning by a plug-in in The Bat!" on page 59) are configured directly in The Bat! and override the application’s email protection settings.

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

SEE ALSO

Mail Anti-Virus 54

CHANGING SECURITY LEVEL

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

- If you work in a non-secure environment, the high security level will suit the best to your email. An example of such environment is a connection to a free email service, from a network that is not guarded by centralized email protection.
- Recommended level provides an optimum balance between efficiency and security, being suitable for most cases. This is also the default setting.
- If you work in a well secured environment, low security level can be used. An example of such an environment might be a corporate network with centralized email security.

If none of the preset levels meet your needs, you can modify Mail Anti-Virus settings on your own (see section "Mail Anti-Virus" on page 54). As a result, the security level's name will change to **Custom**. To restore the default component's settings, select one of the preset security levels.

➧ *To change the preset email security level:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.
4. Select the required security level in the window that will open.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

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

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

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

By default, upon detection of a dangerous of potentially infected object, Mail Anti-Virus displays a warning on the screen and offers a choice of several actions for the object.

All possible actions are shown in the table below.

IF THE ACTION SELECTED WAS	WHEN A DANGEROUS OBJECT IS DETECTED
● **Prompt for action**	Mail Anti-Virus will issue a warning message containing information about what malicious program has infected (potentially infected) the file, and gives you the choice of one of the following actions.
● **Block access**	Mail Anti-Virus will block access to the object. Relevant information is logged in the report. Later you can attempt to disinfect this object.
● **Block access** ☑ **Disinfect**	Mail Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object could not be disinfected, it is placed to Quarantine. Relevant information is logged in the report. Later you can attempt to disinfect this object.
● **Block access** ☑ **Disinfect** ☑ **Delete if disinfection fails**	Mail Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be disinfected, it is deleted. A copy of the object will be stored in Backup. Objects with the *potentially infected* status will be placed to Quarantine.
● **Block access** □ **Disinfect** ☑ **Delete**	When Mail Anti-Virus detects an infected or potentially infected object, the component deletes it without informing the user.

Before disinfecting or deleting an object, Mail Anti-Virus creates a backup copy of it, placing the copy to Backup, so that the object could be restored or disinfected in the future.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.
4. Select the required action in the window that will open.

CREATING A PROTECTION SCOPE

Protection scope is understood as the type of messages to be scanned. By default, Kaspersky Anti-Virus scans both incoming and outgoing messages. If only the incoming messages are selected to be scanned, it is recommended to scan the outgoing messages when beginning to work with the application, as your computer may probably contain email worms that use the email as a channel for proliferation. This will avoid unpleasant situations caused by unmonitored mass emailing of infected emails from your computer.

The protection scope also includes:

- Settings for integrating Mail Anti-Virus into the system. By default, the Mail Anti-Virus component is integrated into the Microsoft Office Outlook and The Bat! email client applications.

- Protocols being scanned. Mail Anti-Virus scans email messages being transmitted via the POP3, SMTP, IMAP, and NNTP protocols. Also, the component scans traffic of ICQ and MSN instant messaging clients.

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

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.

4. In the window that will open, click the **Customize** button.

5. In the window that will open, on the **General** tab, in the **Protection scope** section, specify the required values for the settings.

➡ *To specify the integration settings and the protocols being scanned, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.

4. In the window that will open, click the **Customize** button.

5. In the window that will open, on the **General** tab, in the **Integration** section, check the required boxes.

SELECTING THE SCAN METHOD

The scan methods mean checking the links inside the email messages to identify if they are included in the list of suspicious web addresses and / or in the list of phishing addresses.

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

A phishing attack can be disguised, for example, as a letter from your bank with a link to its official website. By clicking the link, you go to an exact copy of the bank's website and can even see the real address in the browser, even though you are actually on a counterfeit site. From this point forward, all your actions on the site are tracked and can be used to steal your money.

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

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

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.

4. In the window that will open, click the **Customize** button.

5. In the window that will open, on the **General** tab, in the **Scan methods** section, check the ☑ **Check if URLs are listed in the base of suspicious web addresses** box.

➧ *To scan links inside the email messages using the database of phishing addresses, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.

4. In the window that will open, click the **Customize** button.

5. In the window that will open, on the **General** tab, in the **Scan methods** section, check the ☑ **Check if URLs are listed in the base of phishing web addresses** box.

EMAIL SCANNING IN MICROSOFT OFFICE OUTLOOK

If you use Microsoft Office Outlook as your mail client, you can set up custom configurations for virus scans.

A special plug-in is integrated in Microsoft Office Outlook when you are installing the application. It allows you to configure Mail Anti-Virus settings quickly, and determine when email messages will be scanned for dangerous objects.

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

➧ *To specify complex filtering conditions:*

1. Open the main Microsoft Outlook application window.

2. Select **Tools** → **Options** from the application menu.

3. On the **Mail Anti-Virus** tab, specify the required email scan mode.

EMAIL SCANNING BY THE PLUG-IN IN THE BAT!

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

The Mail Anti-Virus settings that determine if incoming and outgoing email messages are scanned, as well as actions on dangerous email objects and exclusions, are ignored in case scan of email messages received via POP3, SMTP, IMAP, MAPI and NNTP protocols is disabled. The only thing that The Bat! takes into account is scanning of attached archives.

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

Please remember, incoming email messages are first scanned by Mail Anti-Virus and only after that by The Bat! mail client plug-in. If a malicious object is detected, Kaspersky Anti-Virus will inform you of this. If you select the **Disinfect** (**Delete**) action in the notification window of Mail Anti-Virus, actions aimed at eliminating the threat will be performed by Mail Anti-Virus. If you select the **Skip** action in the notification window, the object will be disinfected by The Bat! plug-in. When sending email messages, the scan is first performed by the plug-in, then by Mail Anti-Virus.

You should decide:

- which stream of email messages will be scanned (incoming, outgoing);

- at what point in time email objects will be scanned (when opening an email message, or before it is saved to the disk);

- the actions taken by the mail client when dangerous objects are detected in emails. For example, you could select:
  - **Try to disinfect infected parts** – try to disinfect the infected email object and, if the object cannot be disinfected, it remains in the email message.
  - **Delete infected parts** – delete the dangerous object in the message, regardless of whether it is infected or suspected of being infected.

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

> The Bat! does not give special headers to emails containing dangerous objects in case scan of email messages received via POP3, SMTP, IMAP, MAPI and NNTP protocols is disabled. If the scan is enabled, messages will be given special headers.

➡ *To set up email protection rules in The Bat!:*

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

USING HEURISTIC ANALYSIS

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

Additionally you can set the detail level for scans: **light**, **medium**, or **deep**. To do so, move the slider bar to the selected position.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.
4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Performance** tab, in the **Scan methods** section, check / uncheck the ☑ **Heuristic analysis** box, and set the detail level for the scan.

SCAN OF COMPOUND FILES

The selection of compound files scan mode affects Kaspersky Anti-Virus performance. You can enable or disable the scan of attached archives and limit the maximum size of objects to be scanned.

➡ *To configure the settings for the scan of compound files:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.

4. In the window that will open, click the **Customize** button.
5. In the window that will open, on the **Performance** tab, select the scan mode for compound files.

ATTACHMENT FILTERING

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

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

➧ *To configure attachment filtering settings:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.
4. In the dropdown menu, click the **Customize** button.
5. In the window that will open, on the **Attachment filter** tab, specify the filtering conditions for email attachments. When you select any of the last two modes, the list of file types will become enabled; there you can specify the required types or add a mask to select a new type.

   If it is necessary to add a mask of a new type, click the **Add** link, and enter the required data in the **File name mask** window that will open.

RESTORING DEFAULT MAIL PROTECTION SETTINGS

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Mail Anti-Virus** component context menu.
4. In the window that will open, click the **Default level** button.

EMAIL PROTECTION STATISTICS

All operations performed by Mail Anti-Virus are recorded in a special report where you can obtain detailed information on the component's operation grouped on tabs:

- All the dangerous objects detected in your email messages by Mail Anti-Virus are listed on the *Detected* tab. The full name and the status assigned by the application when scanning or processing are indicated for each object. If the component has successfully established what malicious program had infected the object, the latter will be assigned the appropriate status: for example, *virus*, *Trojan*, etc. If the type of malicious impact cannot be exactly established, the object is assigned the *suspicious* status. The action applied to the object (detected, not found, disinfected) is also shown next to the status.

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

- The complete list of events that have occurred while using Mail Anti-Virus is kept on the *Events* tab. Events may have the following statuses:

  - *information* (for example, object not processed, skipped by type);
  - *warning* (for example, a virus is detected);
  - *comment* (for example, archive is password-protected).

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

- Scan *statistics* appear on the appropriate tab. Here you will find the total number of email objects scanned, and then in special columns it is separately indicated how many objects out of the total number scanned are archives, how many of them are dangerous, how many have been disinfected, how many quarantined, etc.

- The settings that Mail Anti-Virus is running with are displayed on the *Settings* tab. Use the **Change settings** link to quickly configure the component.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **Mail Anti-Virus** component context menu.

WEB ANTI-VIRUS

Whenever you use the Internet, you impose information stored on your computer to the risk of being infected by dangerous programs. They can penetrate your computer while you are viewing a web page.

Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 includes a special component called *Web Anti-Virus* for ensuring the security to your Internet sessions. It protects your computer against data coming into your computer via the HTTP protocol, and also prevents dangerous scripts from being executed on the computer.

Web protection only monitors HTTP traffic that passes through the ports listed on the list of monitored ports (see section "Creating a list of monitored ports" on page 166). A list of ports that are most commonly used for transmitting email and HTTP traffic is included in the Kaspersky Anti-Virus installation package. If you use ports that are not on this list, you should add them to the list to protect traffic passing via these ports.

If you are working in unprotected space, surfing on the Internet using a modem, it is recommended that you use Firewall to protect yourself while using the Internet. If your computer is running on a network protected by a firewall or by HTTP traffic filters, Firewall will provide additional security when using the Internet.

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

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

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

Kaspersky Lab advises abstaining from configuring Web Anti-Virus on your own. In most cases, selecting a different security level is sufficient.

If Web Anti-Virus has been disabled for any reason, connections established before it had been enabled, will not be monitored. You should restart your browser immediately after Web Anti-Virus is run.

➡ *To edit Web Anti-Virus settings:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

COMPONENT OPERATION ALGORITHM

Web Anti-Virus protects information being received via HTTP, and prevents hazardous scripts from running on the computer.

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

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

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

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

   - If the file or the webpage do not contain malicious code, they will immediately become accessible to the user.

Scripts are scanned according to the following algorithm:

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

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

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

A special plug-in is provided for Microsoft Internet Explorer; it is integrated into the browser when installing the application. It is available when a new button appears in the browser's toolbar. Clicking it opens an information panel with Web Anti-Virus statistics on the number of scripts scanned and blocked.

SEE ALSO

Web Anti-Virus 63

CHANGING HTTP TRAFFIC SECURITY LEVEL

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

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

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

➡ *To change the preset security level for web traffic:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. Select the required security level in the window that will open.

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

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

Web Anti-Virus always blocks actions by dangerous objects and issues pop-up messages that inform the user about the action taken.

Let's look at the possible options for processing dangerous HTTP objects in more detail.

IF THE ACTION SELECTED WAS	IF A DANGEROUS OBJECT IS DETECTED IN THE HTTP TRAFFIC
◉ **Prompt for action**	Web Anti-Virus will issue a warning message containing information about what malicious code has potentially infected the object and will give you a choice of responses.
◉ **Block**	Web Anti-Virus will block access to the object and will display a message on screen about blocking it. Similar information will be recorded in the report.
◉ **Allow**	Web Anti-Virus will grant access to the object. Relevant information is logged in the report.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. Select the required action in the window that will open.

CREATING A PROTECTION SCOPE

Protection scope is a list of trusted addresses which will not be scanned for viruses by the protection component. Option of creating such a list may be useful, for instance, when Web Anti-Virus interferes with downloading a particular file.

➡ *To create the list of trusted addresses:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, click the **Customize** button.
5. In the **Custom Settings: Web Anti-Virus** window that will open, in the **Trusted URLs** section, click the **Add** button.
6. In the **Address mask (URL)** window that will open, enter a trusted address (or its mask).

SELECTING THE SCAN METHOD

The scan methods mean checking the links to identify if they are included in the list of suspicious addresses and / or in the list of phishing addresses.

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

Since the link to a phishing site can be received not only in an email message (see section "Selecting the scan method" on page 58) but in any other way, for example, in the text of an ICQ message, the Web Anti-Virus component traces the attempts of accessing a phishing site at the level of HTTP traffic scan, and blocks it.

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, click the **Customize** button.
5. In the **Custom Settings: Web Anti-Virus** window that will open, in the **Scan methods** section, check the ☑ **Check if URLs are listed in the base of suspicious web addresses** box.

➡ *To scan links using the database of phishing addresses, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, click the **Customize** button.
5. In the **Custom Settings: Web Anti-Virus** window that will open, in the **Scan methods** section, check the ☑ **Check if URLs are listed in the base of phishing web addresses** box.

USING HEURISTIC ANALYSIS

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

Kaspersky Anti-Virus will notify you when a malicious object is detected in a message. You should react to the notification by selecting an action.

Additionally you can set the detail level for scans: **light**, **medium**, or **deep**. To do so, move the slider bar to the selected position.

➡ *To use the heuristic analysis and to set the detail level for scans, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, click the **Customize** button.
5. In the **Custom Settings: Web Anti-Virus** window that will open, in the **Scan methods** section, check the ☑ **Heuristic analysis** box and specify the scan detail level below.

SCAN OPTIMIZATION

To detect malicious code more efficiently, Web Anti-Virus buffers fragments of objects downloaded from the Internet. When using this method, Web Anti-Virus scans an object only after it has been completely downloaded. The object is then analyzed for viruses and, depending on the outcome, the application returns the object to the user or blocks it.

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

To solve this problem, we suggest limiting the buffering time for web object fragments downloaded from the Internet. When this time limit expires, the user will receive the downloaded part of the file without scanning, and once the object is fully copied, it will be scanned in its entirety. This helps shorten the time of object delivery to user, and also solves the problem of interrupted Internet connections without lowering Internet security level.

By default, the buffering time for file fragments is limited to one second. Increasing this value or switching off the caching time limit will lead to more efficient virus scans, but somewhat slower delivery of the object.

➡ *To limit the caching time for file fragments:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, click the **Customize** button.
5. In the **Custom Settings: Web Anti-Virus** window that will open, in the **Scan optimization** section, check the ☑ **Limit fragment caching time** box and enter the time value (in seconds) in the field next to it.

RESTORING DEFAULT WEB PROTECTION SETTINGS

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

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Web Anti-Virus** component context menu.
4. In the window that will open, click the **Default level** button.

WEB ANTI-VIRUS STATISTICS

General information about the Web Anti-Virus functioning is saved in a special report where you can find a detailed report on the component functioning, grouped by tabs:

- All the dangerous objects detected by Web Anti-Virus in the HTTP traffic are shown on the *Detected* tab. The name of the object and the name of the dangerous object are shown here. For this tab not to contain information about disinfected HTTP traffic objects, uncheck the ☑ **Show disinfected objects** box.
- The complete list of events that have occurred while using Web Anti-Virus is kept on the *Events* tab. All events can be divided in important events and minor notifications. As a rule, the minor notifications are of a reference nature and are not of particular interest. You can disable display of such events. To do so, uncheck the ☑ **Show all events** box.
- The settings Web Anti-Virus is running with are displayed on the *Settings* tab. Use the **Change settings** link to quickly configure the component.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **Web Anti-Virus** component context menu.

PROACTIVE DEFENSE

Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 protects you both from known threats and from new ones on which there is no information in the application databases. This is ensured by the *Proactive Defense* component.

The preventative technologies provided by Proactive Defense allow to save time and neutralize new threats before they harm your computer. How is this done? In contrast with reactive technologies, which analyze code based on records in the application databases, preventative technologies recognize a new threat by the sequence of actions executed by a harmful program. The program includes a set of criteria that can determine how dangerous the activity of a program is. If analysis of a sequence of actions makes the program suspicious, Kaspersky Anti-Virus takes the action assigned by the rule for that type of activity.

Dangerous activity is defined by the overall actions of the program. Dangerous activity includes:

- changes to the file system;
- modules being imbedded in other processes;
- masking processes in the system;
- changes to certain Microsoft Windows system registry keys.

Proactive Defense is carried out in strict correspondence with settings that define:

- *Whether application activity is subject to monitoring on your computer*. This Proactive Defense mode is ensured by the **Application Activity Analyzer** module. By default this mode is enabled, which ensures that the actions of any programs opened on your computer will be closely tracked.
- *Whether system registry changes are monitored*. This Proactive Defense mode is ensured by the **Registry Guard** module. By default, the module is disabled, which means the Kaspersky Anti-Virus doesn't analyze attempts to make changes to the Microsoft Windows system registry keys.

➧ *To edit Proactive Defense settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

COMPONENT OPERATION ALGORITHM

The preventative technologies provided by Kaspersky Anti-Virus's Proactive Defense recognize a new threat on your computer by a sequence of actions executed by a certain program. Kaspersky Anti-Virus installation package includes a set of criteria that can determine how dangerous the activity of an application is. If analysis of a sequence of actions considers an application suspicious, Kaspersky Anti-Virus takes the action specified in the rule for dangerous activity.

Let us take a closer look at the Proactive Defense's algorithm.

1. Immediately after the computer is started, Proactive Defense analyzes the following factors:

   - *Actions of each application running on the computer*. Proactive Defense records the history of actions taken in order and compares them to sequences typical of dangerous activity (a database of dangerous activity types is included in the application installation package and is updated together with the application databases).

   - *Each attempt of editing the system registry* by deleting or adding system registry keys, entering inappropriate values for keys impacting viewing and editing, etc.

2. The analysis is based on the allow and block rules of Proactive Defense.

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

   - If the activity meets the conditions of the Proactive Defense allow rule or does not match any block rule, it will not be blocked.

   - If a block rule covers the activity, the component's further steps will be determined by the instructions specified in the rule. Such activity is usually blocked. A notification will be displayed on the screen specifying the application, its activity type, and the history of actions taken. You should make a decision on whether you want to block, or to allow this activity. You can create a rule for such activity and cancel the actions taken in the system.

SEE ALSO

Proactive Defense 70

APPLICATION ACTIVITY ANALYZER

The **Application Activity Analyzer** component of Kaspersky Anti-Virus monitors applications' activity on your computer. The application includes a set of event descriptions that can be regarded as dangerous. A monitoring rule is created for each such event. If the activity of any application is classified as a dangerous event, Proactive Defense will strictly adhere to the instructions stated in the rule for that event.

SEE ALSO

Using the list of dangerous activity 71

Changing the dangerous activity monitoring rule...72

System accounts control 73

Proactive Defense events...73

USING THE LIST OF DANGEROUS ACTIVITY

Note that configuring application control under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64 differs from the configuration process applied to an application running under other operating systems.

Specifics of configuring application activity control under Microsoft Windows XP

Kaspersky Anti-Virus monitors application activity on your computer. Proactive Defense reacts immediately to a defined sequence of application actions. Hazardous sequences of actions include the following:

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

The list of dangerous activities is added to automatically when Kaspersky Anti-Virus is updated, and it cannot be edited. However, you can disable monitoring for one dangerous activity or another.

➡ *To turn off monitoring for one dangerous activity or another:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Application Activity Analyzer** section, click the **Settings** button.
5. In the **Settings: Application Activity Analyzer** window that will open, uncheck the ☑ box next to the name of the activity which you do not want to be monitored.

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

If the computer is running under one of the above-mentioned operating systems, then control will not apply to each event; this is due to particular features of these operating systems.

CHANGING THE DANGEROUS ACTIVITY MONITORING RULE

The list of dangerous activities is added to automatically when Kaspersky Anti-Virus is updated, and it cannot be edited. You can:

- turn off monitoring for one dangerous activity or another (see page 71);
- edit the rule that Proactive Defense uses when it detects dangerous activity;
- create an exclusion list (see page 146) by listing the applications with activity that you do not consider dangerous.

To change the rule:

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Application Activity Analyzer** section, click the **Settings** button.
5. In the **Settings: Application Activity Analyzer** window that will open, in the **Events** section, select the required event for which you want to change the rule.
6. Configure the rule for the selected event, using the links in the description section:
   - click the link with the preset action and select the required action in the **Select action** window that will open;
   - click the link with the preset time period (not for any activity type), and specify the scan interval for hidden processes in the **Hidden processes detection** window that will open;
   - click the **on / off** link to indicate that the report on task execution should be created.

SYSTEM ACCOUNTS CONTROL

User accounts control access to the system and identify the user and his/her work environment, which prevents other users from corrupting the operating system or data. System processes are processes launched by system user accounts.

If you want Kaspersky Anti-Virus to monitor the activity of system processes in addition to user processes:

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Application Activity Analyzer** section, click the **Settings** button.
5. In the **Settings: Application Activity Analyzer** window that will open, in the **General** section, check the ☑ **Monitor system user accounts** box.

PROACTIVE DEFENSE EVENTS

This section provides you with information about the Proactive Defense events which may be treated as dangerous. Please note that each event should not be unambiguously interpreted as a treat. Some of those operations are part of the common behavior of applications running on the computer, or they may be taken as a reaction of the operating system to the functional features of the applications. However, in some cases those events may turn out to be caused by an intruder's activity or by a malicious program. So, it is important to realize that Proactive Defense's triggering does not necessarily indicate that the activity it has detected had been caused by a malicious program: this may also be a common harmless program featuring certain traits of a malicious one.

Activity typical of P2P worms / Activity typical of Trojans

Worm is a self-replicating program spreading via computer networks. P2P worms spread in the "computer-to-computer" way, bypassing centralized management. As a rule, such worms spread via shared network folders and removable media.

Trojan is a malicious program that penetrates into the computer in the guise of a harmless one. Hackers upload Trojans to open network resources, data media available for recording on a computer, removable media, and distribute them using messaging services (such as email) to run them on the computer.

Typical activity of such programs includes the following:

- actions typical of a malicious object penetrating and implanting in the system;
- malicious actions as such;
- actions typical of a malicious object spreading.

Keyloggers

Keylogger is a program that intercepts each keypress at the keyboard. Such a malicious program can send any information entered at the keyboard (logins, passwords, credit card numbers) to an intruder. However, keypress interception may be used by common legal programs. An example of such programs is a video game that has to intercept data entered at the keyboard to be aware of keys being pressed by the user, when functioning in full-screen mode. Also, keypress interception is often used to activate a program's function from another program using "hotkeys".

Hidden driver installation

Hidden driver installation is a process of installing a malicious program's driver in order to obtain low-level access to the operating system which may allow concealing the malicious program persisting in the system and complicating its removal. Hidden installation process can be detected using common means (such as Microsoft Windows Task Manager), but since no standard installation windows appear during the driver installation, the user can hardly suspect that he or she should track the processes running within the system.

However, in some cases Proactive Defense may return a false alert. For example, the most recent video games are protected against unauthorized copying and distribution. With that end in view, they install system drivers on the user's computer. Such activities may be classified as "hidden driver installation" in some cases.

Modifying the operating system kernel

The operating system kernel grants the applications running on the computer a coordinated access to the computer's resources: CPU, RAM, and external hardware. Some malicious programs can attempt to change the operating system kernel's logic, by redirecting queries from standard drivers to itself. When malicious programs obtain the low-level access to the operating system in that way, they attempt to conceal their presence and complicate the process of removing them from the system.

An example of a false alert returned by Proactive Defense is the component's reaction to certain encryption systems designed for hard disk drives. Those systems designed to ensure comprehensive data protection install a driver into the system, implanting into the operating system kernel in order to intercept queries to the files on the hard drive, and to perform encryption/decryption operations.

Hidden object / Hidden process

Hidden process is a process that cannot be detected by common means (such as Microsoft Windows Task Manager, Process Explorer, etc.). Rootkit (i.e. "kit designed to obtain root privileges") is a program or a collection of programs for the hidden control of a hacked system. This term has been imported from Unix.

In the scope of Microsoft Windows, rootkit usually means a masking program that implants into the system, intercepts and falsifies system messages containing the information about the processes running in the system and about the content of folders on the disk drive. In other words, a rootkit functions similarly to a proxy server, as it lets certain data flow intact while blocking or falsifying the rest of data. Also, a rootkit can usually mask the presence of any processes, folders and files stored on a disk drive, and registry keys, if they are described in its configuration. Many masking programs install their own drivers and services into the system, making them "invisible" both to system management tools (such as Task Manager or Process Explorer), and to anti-virus applications.

A particular case of hidden process is an activity consisting in attempting to create hidden processes with negative PID values. PID is the personal identification number that the operating system assigns to each running process. PID is unique for each running process, it is only static for each one in the current session of the operating system. If the PID of a process has a negative value, this process is hidden, so it cannot be detected using common means.

An example of a false alert is the triggering of Proactive Defense reacting to gaming applications which protect their own processes against hacking utility tools designed to evade license restrictions or cheat.

Modifying HOSTS file

Hosts file is one of the most important system files of Microsoft Windows. It is designed to redirect access to web resources by converting URL addresses into IP addresses not at DNS servers but strictly on a local computer. Hosts file is a plain text file, where each line determines the matching between the symbol name (URL) of a server and its IP address.

Malicious programs often use that file for redetermining addresses of update servers for anti-virus applications to block updates and prevent the detection of malicious programs with the signature method, and for other purposes.

Redirecting input-output

The essential weak point consists in running a command line with redirected input/output (usually, into the network), which, as a rule, can be used to obtain remote access to the computer.

A malicious object attempts to obtain access to the command line of a target computer, which will then be exploited to execute commands. Access may usually be obtained after a remote attack and the launch of a script that uses this vulnerability. The script runs the command line interpreter from the computer connected via TCP. As a result, the intruder can manage the system remotely.

Intruding into a process / Intruding into all processes

There are many types of malicious programs that are masked as executable files, libraries or extension modules of known programs, intruding into standard processes. So, an intruder can make a data loss on the user's computer. Network traffic created by malicious code will not be filtered out by firewalls, since it is viewed by them as traffic created by a program that has been granted Internet access.

Trojans usually intrude into other processes. However, such activities are also typical of certain harmless programs, update packages, and installation wizards. For example, translation programs intrude into other processes to track the presses of hotkeys.

Suspicious access to the registry

Malicious programs modify the registry in order to record themselves for autorun at the operating system startup, change the home page in Microsoft Internet Explorer, and take many other destructive actions. However, please note that the system registry may also be accessed by common programs. For example, common programs may use the option of creating and exploiting hidden registry keys to conceal their own confidential information (including license information) from the user.

Malicious programs create hidden registry keys that are not displayed by common programs (regedit-type). Keys with invalid names are created. This is done in order to prevent the registry editor against displaying those values, which results in complicating the diagnostics of malware presence within the system.

Sending data using trusted applications

There are many types of malicious programs that are masked as executable files, libraries or extension modules of known programs, intruding into standard processes. So, an intruder can make a data loss on the user's computer. Network traffic created by malicious code will not be filtered out by firewalls, since it is viewed by them as traffic created by a program that has been granted Internet access.

Suspicious activity in the system

This point consists in detecting a suspicious behavior of a separate process: a change in the operating system's status, for example, granting direct access to the RAM, or obtaining debugger privileges. Intercepted activity is not typical for the most programs, being dangerous at the same time. So, such activity is classified as suspicious.

Sending DNS requests

DNS server is designed to reply to DNS requests via the corresponding protocol. If no record matching the DNS request is found in the local DNS server's database, the request will be retransmitted, until it reaches a server that would store the required information. As DNS requests are let flow by the most protection systems without scanning, the content of a DNS package may include additional fragments containing the user's personal data. An intruder controlling a DNS server that processes those DNS requests, has an opportunity to obtain this information.

Attempting to access a protected storage

A process attempts to obtain access to a protected storage within the operating system containing the user's personal data and passwords.

REGISTRY GUARD

One of the goals of most malicious programs is to edit the operating system's registry on your computer. These can be harmless joke programs or more dangerous malicious programs that impose a real threat on your computer.

For example, malicious programs can copy their information to the registry key that makes applications open automatically at startup. As a result, malicious programs will automatically be started when the operating system boots up.

Changes in registry objects are monitored by the dedicated Proactive Defense module named **Registry Guard**.

SEE ALSO

MANAGING THE LIST OF SYSTEM REGISTRY MONITORING RULES

Kaspersky Lab has already created a list of rules that control operations with registry objects, and has included it in the application installation package. Operations with registry objects are divided into logical groups, such as *System Security*, *Internet Security*, etc. Each of these groups includes system registry objects and rules for working with them. This list is updated together with the entire application.

Each group of rules has an execution priority that you can raise or lower. The higher the group is on the list, the higher execution priority is assigned to it. If the same registry object falls under several groups, the first rule applied to the object will be the one from the group with higher priority.

➡ *To raise or lower the execution priority for a rule, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Registry Guard** section, click the **Settings** button.
5. In the **Settings: Registry Guard** window that will open, use the **Move up** / **Move down** buttons.

➡ *To stop using any group of rules, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Registry Guard** section, click the **Settings** button.

5. In the **Settings: Registry Guard** window that will open, uncheck the ☑ box next to the group's name. In this case, the group of rules will remain on the list but will not be used. It is not recommended to delete the group of rules from the list, since it contains a list of system registry objects most often used by malicious programs.

CREATING A GROUP OF SYSTEM REGISTRY OBJECTS TO MONITOR

You can create your own groups of monitored system registry files.

➡ *To create a group of controlled system registry objects:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Registry Guard** section, click the **Settings** button.
5. In the **Settings: Registry Guard** window that will open, click the **Add** button.
6. In the window that will open enter the name of the new group for monitoring system registry objects in the **Group name** field.

   Create a list of objects from the system registry that the group will include on the **Keys** tab.

   On the **Rules** tab, create a rule for the selected system registry objects.

SEE ALSO

Selecting registry objects for creating a rule 77

Creating a rule for monitoring registry objects 78

SELECTING REGISTRY OBJECTS FOR CREATING A RULE

The group of objects being created should contain at least one system registry object.

➡ *To add a system registry object to the list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Registry Guard** section, click the **Settings** button.
5. In the **Settings: Registry Guard** window that will open, click the **Add** button.
6. In the window that will open, on the **Keys** tab, click the **Add** button.
7. In the **Please specify a registry object** window that will open, please do the following:

   a. select a system registry object or a group of objects for which you wish to create a monitoring rule;

   b. specify the object value or a mask for a group of objects that you wish the rule to apply to, in the **Value** field;

c. if you wish the rule to apply to all embedded keys for the selected system registry object, check the ☑ **Include subkeys** box.

CREATING A RULE FOR MONITORING REGISTRY OBJECTS

A system registry objects monitoring rule consists in determining the following:

- the application to which the rule will be applied if it attempts to access the system registry;
- the program's reaction to an application attempting to perform an operation with the system registry.

➧ *To create a rule for the selected system registry objects, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Proactive Defense** component context menu, select the **Settings** item.
4. In the window that will open, in the **Registry Guard** section, click the **Settings** button.
5. In the **Settings: Registry Guard** window that will open, click the **Add** button.
6. In the window that will open, on the **Rules** tab, click the **New** button. The general rule will be added as the first on the rule list.
7. Select a rule on the list and specify the rule settings in the bottom part of the tab:

   - Specify the application.

     By default, a rule is created for each application. If you want a rule to apply to a specific application, left-click on **Any**, and it will change to **Selected**. Then use the **specify application name** link. A context menu will open, where you can go to the standard file selection window from the **Browse** item, or go to the list of applications currently running from the **Applications** item, and select the ones you need.

   - Specify the Proactive Defense's reaction to the selected application attempting to read, edit, or delete system registry objects.

     You can use any of the following actions as a reaction: **allow**, **prompt for action**, and **block**. Left-click on the link with the action until it reaches the value you need.

   - Specify if it is necessary to generate a report of the performed operation. To do so, click the **log** / **do not log** link.

   You can create several rules and rank their priority using the **Move up** and **Move down** buttons. The higher position in the list the rule has, the higher priority it has.

PROACTIVE DEFENSE STATISTICS

All operations performed by Proactive Defense are recorded in a special report where you can obtain detailed information on the component's operation grouped on the following tabs:

- *Detected* – all objects classified as dangerous are collected on this tab.
- *Events* – events related to monitoring application activity are listed on this tab.
- *Registry* – this tab contains all operations involving the system registry.
- *Settings* – on this tab you can find the settings regulating the functioning of Proactive Defense.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Report** item from the **Proactive Defense** component context menu. You can select the type of information on each report tab, sort it in ascending and descending order for each column, and search for information in the report. To do so, use the items of the context menu which you can open by right-clicking on the headings of report columns.

ANTI-SPY

Recently, malware has come to include more and more programs that aim to:

- obtrusively deliver advertising content in web browsers, pop-up windows, and banners in various programs;
- make attempts of unauthorized modem connections.

Keyboard interceptors focus on stealing your information; auto-dialers, joke programs, and adware aim to waste your time and money. Protecting you from these programs is what *Anti-Spy* is designed to do.

Anti-Spy includes the following modules:

- *Anti-Banner (see page 80)* blocks advertisements on special banners on the web or built into the interfaces of various programs installed on your computer;
- *Anti-Dialer (see page 82)* – prevents attempts to make unauthorized modem connections.

➡ *To edit Anti-Spy settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Anti-Spy** component context menu, select the **Settings** item.
4. In the window that will open make the required changes in the component modules settings.

IN THIS SECTION

ANTI-BANNER

Anti-Banner blocks advertisements on special banners on the web or built into the interfaces of various programs installed on your computer.

Banner ads are not only devoid of useful information. They distract you from your work and increase the amount of traffic on your computer. Anti-Banner blocks the most common banner ads. Kaspersky Anti-Virus includes masks for this purpose. You can disable banner blocking or create your own lists of allowed and blocked banners.

To integrate the Anti-Banner module into the **Opera** browser, add the following line into the *standard_menu.ini* file, **[Image Link Popup Menu]** section: Item, "New banner" = Copy image address & Execute program, "<drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations MP4\opera_banner_deny.vbs", "//nologo %C". Specify the name of your system disk drive instead of <drive>.

SEE ALSO

CREATING THE LIST OF ALLOWED BANNER ADDRESSES

A user creates the white list of banners while working with the application if a necessity occurs to exclude certain banners from blocking. This list contains masks for allowed banner ads.

➧ *To add a new mask to the white list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Anti-Spy** component context menu, select the **Settings** item.
4. In the window that will open, in the **Anti-Banner** section, click the **Settings** button.
5. In the window that will open, on the **White List** tab, click the **Add** button.
6. Enter a mask of an allowed banner in the **Address mask (URL)** window that will open. To stop using a mask that you created, you do not have to delete it from the list; unchecking the box ☑ next to it renders it inactive.

CREATING THE LIST OF BLOCKED BANNER ADDRESSES

You can create a list of banned banner addresses which will be blocked by Anti-Banner when detected.

➧ *To add a new mask to the "black" list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Anti-Spy** component context menu, select the **Settings** item.
4. In the window that will open, in the **Anti-Banner** section, click the **Settings** button.
5. In the window that will open, on the **Black List** tab, click the **Add** button.
6. Enter the mask of a blocked banner in the **Address mask (URL)** window that will open. To stop using a mask that you created, you do not have to delete it from the list; unchecking the box ☑ next to it renders it inactive.

ADVANCED COMPONENT SETTINGS

Kaspersky Lab's specialists have compiled a list of banner ad masks based on a specially conducted research, and have included it with the Kaspersky Anti-Virus installation package. Banner ads that match the masks on the list, will be blocked by the application unless banner blocking is disabled.

When creating the lists of allowed / banned banners, either banner's IP address or its symbol name (URL) may be entered. To avoid dubbing, you can use an advanced option which allows converting IP addresses into domain names, and vice-versa.

➡ *To disable the use of the list of banners included in the application installation package, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Anti-Spy** component context menu, select the **Settings** item.
4. In the window that will open, in the **Anti-Banner** section, click the **Settings** button.
5. In the window that will open, on the **Additional** tab, check the ☑ **Do not use common banners list** box.

➡ *To use the option of converting banners' IP addresses into domain names (or domain names into IP addresses), please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Anti-Spy** component context menu, select the **Settings** item.
4. In the window that will open, in the **Anti-Banner** section, click the **Settings** button.
5. In the window that will open, on the **Additional** tab, check the ☑ **Resolve IP addresses to domain names** box.

EXPORTING / IMPORTING BANNER LISTS

You can copy the lists of allowed / blocked banners you have created from one computer to another. While exporting the list, you can copy either the selected list element only, or the entire list. While importing the list, you can choose to add the new addresses to the existing list, or replace the existing list with the one being imported.

➡ *To copy the created lists of allowed / blocked banners, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. In the **Anti-Spy** component context menu, select the **Settings** item.
4. In the window that will open, in the **Anti-Banner** section, click the **Settings** button.
5. In the window that will open, on the **White List** tab (or on the **Black List** tab), use the **Import** or **Export** buttons.

ANTI-DIALER

Anti-Dialer protects you from unauthorized attempts to make connections via your modem. A connection is considered secret if it is configured not to inform the user of the connection, or if it is a connection that you do not initiate. As a rule, secret connections are established to commercial phone numbers.

Whenever a secret connection is attempted, you will be notified of it with a special message displayed on the screen. It requires you to allow or block the connection. If you have not initiated that connection, it is highly likely that this occurred due to a malicious program. If you wish to allow hidden dialing to a certain number, you should include this number in the list of trusted numbers.

➧ *To add a number to the list of trusted numbers, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. In the **Anti-Spy** component context menu, select the **Settings** item.

4. In the window that will open, in the **Anti-Dialer** section, click the **Settings** button.

5. In the **Settings: Trusted numbers** window that will open, click the **Add** button.

6. In the **Phone number** window that will open, specify a trusted number or a mask.

ANTI-SPY STATISTICS

A detailed description of all operations on protection against Internet fraud is given in a special report. All events are sorted by various tabs depending on which Anti-Spy module they were tracked with:

- The *Banners* tab displays banner ads detected and blocked during the current session of the application.

- All the attempts of malicious programs to connect your computer to paid telephone numbers are recorded on the *Hidden dials* tab.

- On the *Settings* tab, you can find the settings regulating the functioning of Anti-Spy.

➧ *To view information about the component's operation, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Report** item from the **Anti-Spy** component context menu. You can select the type of information on each report tab, sort it in ascending and descending order for each column, and search for information in the report. To do so, use the items of the context menu which you can open by right-clicking on the headings of report columns.

PROTECTION AGAINST NETWORK ATTACKS

Kaspersky Anti-Virus comprises the special *Anti-Hacker* component to ensure your security on local networks and on the Internet. It protects your computer on the network and application level and masks your computer on the network to prevent attacks.

Based on the two Anti-Hacker protection levels, there are two rule types:

- *Rules for packet filtering*. Used to impose general restrictions on network activity, regardless of the applications installed. For example: if you create a packet rule that blocks inbound connections to Port 21, no applications that use that port (an FTP server, for example) will be accessible from the outside.

- *Rules for applications*. Used to impose restrictions on network activity for specific applications. For example: if connections to Port 80 are blocked for each application, you can create a rule that allows connections to that port for Firefox browser only.

There are two types of rules which *allow* or *block* some applications and network packets. Kaspersky Anti-Virus installation package includes a set of rules that regulate network activity for the most common applications and using the most common protocols and ports. Kaspersky Anti-Virus installation package also includes a set of allow rules for trusted applications whose network activity is not cause for suspicion.

To make settings and rules user-friendlier, Kaspersky Anti-Virus breaks down the entire network space into security zones, which largely correspond to the subnetworks that your computer belongs to. You can assign a status to each zone (*Internet*, *Local Network*, *Trusted*), which will determine the policy for applying rules and network activity monitoring in that zone.

A special feature of Anti-Hacker, called Stealth Mode, prevents the computer from being detected from the outside. Thus, the hackers lose the object of attack. This mode does not affect your computer's performance on the Internet (under condition that your computer is not used as a server).

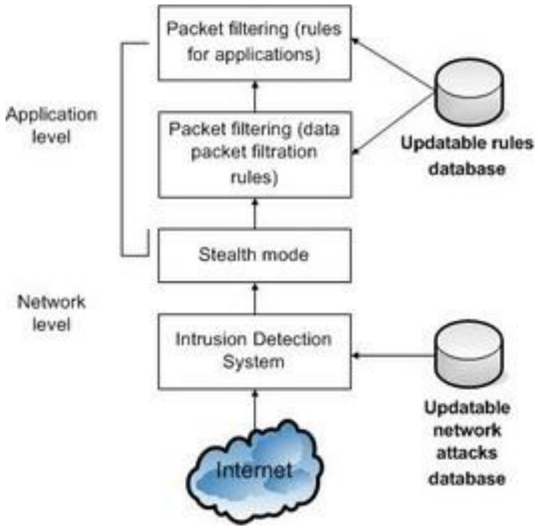
➡ *To edit Anti-Hacker settings, please do the following*:

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

COMPONENT OPERATION LAYOUT

Anti-Hacker protects your computer at the network and application levels, and masks your computer on the network to prevent attacks. Let us take a closer look at Anti-Hacker's principles of operation.


Packet filtering (rules for applications)
Application level
Packet filtering (data packet filtration rules)
Updatable rules database
Stealth mode
Network level
Intrusion Detection System
Updatable network attacks database
Internet

You are protected at the network level by using global packet filtration rules where network activity is allowed or blocked based on analyzing such settings as packet transfer direction, data packet transfer protocol, and outbound packet port. Rules for packets regulate access to the network, regardless of the applications installed on your computer that use the network.

In addition to the packet filtering rules, the *Intrusion Detection System (IDS)* provides additional security on the network level (see section "Intrusion detection system" on page 96). The purpose of the subsystem is to analyze inbound connections, detect port scans on your computer, and filter network packets aimed at exploiting software vulnerabilities. When running, the Intrusion Detection System blocks all inbound connections from an attacking computer for a certain amount of time, and the user receives a message stating that his or her computer underwent a network attack.

The Intrusion Detection System's functioning is based on using a special database of network attacks (see section "Types of network attacks" on page 96) in analysis, which is regularly enlarged by Kaspersky Lab's specialists. It is updated together with the application databases.

Your computer is protected on the application level by applying application rules for using network resources to the applications installed on your computer. Like the network protection level, the application protection level is built on analyzing data packets for direction, transfer protocol, and what ports they use. However, at the application level, the program takes into account the features of both the data packet and the specific application that sends and receives the packet.

Using application rules helps you configure more specific protection features when, for example, a certain connection type is banned for some applications but not for others.

SEE ALSO

Protection against network attacks 84

CHANGING ANTI-HACKER PROTECTION LEVEL

When you use the network, Kaspersky Anti-Virus protects your computer at one of the following levels:

- **High Security** – security level at which the network activity is allowed as far as is stipulated by an allow rule. Anti-Hacker uses the rules included with the application installation package, or those you have created. The set of rules shipped with Kaspersky Anti-Virus includes allow rules for applications whose network activity is not suspicious, and for data packets which are absolutely safe to send and receive. However, if there is a block rule in the list of rules for an application with higher priority than the allow rule, Kaspersky Anti-Virus will block the network activity of that application.

  > If you select this protection level, any network activity not recorded in Anti-Hacker allow rules will be blocked. Therefore we recommend only using this level if you are certain that all the programs that you need are allowed by the rules and that you do not intend to install new software.
  >
  > Note that Microsoft Office Outlook functioning may be hindered at this level. If the mail client processing incoming messages use its own rules, mail delivery will fail since the mail client will not be allowed to access to Exchange server, at this level of protection against network attacks. The same case may occur if the user's mailbox has been transferred to a new Exchange server. To resolve such problems, an allowing rule for Microsoft Office Outlook should be created (or changed if such a rule has been created earlier); it should allow any activities at IP address of Exchange server.

- **Training Mode** – level of protection at which Anti-Hacker rules are created. At this level, every time a program attempts to use a network resource, Anti-Hacker checks to see if there is a rule for that connection. If there is a rule, Anti-Hacker follows its instructions. If no rule has been created, it displays a description of the network connection (what program has initiated it, via what port and protocol, etc.). You should decide whether you should allow this connection or not. By using a special button in the notification window, you can create a rule for that connection so that in the future Anti-Hacker will use the conditions in the rule for that connection without notifying you on the screen.

- **Low Security** blocks only clearly banned network activity. Anti-Hacker blocks the activity in accordance with block rules included with the application installation package, or those you have created. However, if there is an allow rule in the list of rules for an application with higher priority than the block rule, Kaspersky Anti-Virus will allow the network activity of that application.

- **Allow All** – protection level at which all network activity on your computer is allowed. We recommend setting protection at this level in a few special cases when no active network attacks have been observed and you fully trust all network activity.

You can raise or lower the network protection level, by selecting the level you want, or by editing the settings for the current level.

➡ *To change the network attack protection level, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, select the required level of protection against network attacks.

RULES FOR APPLICATIONS AND PACKET FILTERING

Firewall rule is an action performed by Firewall once it detects a connection attempt with certain settings. You can create:

- Packet rules. Packet rules are used for imposing restrictions on data packets and streams irrespective of the applications.
- Rules for applications. Rules for applications are used for imposing restrictions on the network activity of a certain application. Such rules allow fine-tuning the filtering, for example, when a certain type of data stream is banned for some applications but is allowed for other ones.

SEE ALSO

RULES FOR APPLICATIONS. CREATING A RULE MANUALLY

Kaspersky Anti-Virus installation package includes a set of rules for the most widespread applications running under Microsoft Windows. You can create several allowing or blocking rules for the same application. These would generally be applications with network activity that has been thoroughly analyzed by Kaspersky Lab and strictly defined as dangerous or safe.

Depending on the protection level selected for Firewall, and on the type of network the computer is running on, the list of rules can be used in various ways. Thus, for example, at the **High Security** level, all network activity of applications not covered by allowing rules, is blocked.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.

5. In the window that will open, on the **Rules for applications** tab, click the **Add** button. A context menu will open, where you can go to the standard file selection window by selecting the **Browse** item, or go to the list of applications currently running by selecting the **Applications** item, and select the ones you need. A list of rules for the selected application will open. If rules for it already exist, they all will be listed in the top part of the window. If no rules exist, the rules window will be empty.

6. Click the **Add** button in the rules window for the application selected.

7. The **New rule** window that will open provides a rule creation form that you can use to fine-tune a rule.

RULES FOR APPLICATIONS. CREATING RULES WITH TEMPLATES

Kaspersky Anti-Virus includes ready-made rule templates that you can use when creating your own rules.

The entire spectrum of existing network applications may be divided into a few types: mail clients, web browsers, etc. Each type has a set of specific activities, such as email reception and sending, or downloading and displaying of HTML pages. Each type uses a certain set of network protocols and ports. This is why having rule templates helps you quickly and easily make initial configurations for rules based on the type of application.

➧ *To create an application rule using a rule template as a basis, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Anti-Hacker** component context menu.

4. In the window that will open, in the **Firewall** section, click the **Settings** button.

5. In the window that will open, on the **Rules for applications** tab, check the ☑ **Group rules by application** box unless it is already checked, and click the **Add** button. A context menu will open, where you can go to the standard file selection window by selecting the **Browse** item, or go to the list of applications currently running by selecting the **Applications** item, and select the ones you need. A window with rules for the selected application will open. If rules for it already exist, they all will be listed in the top part of the window. If no rules exist, the rules window will be empty.

6. Click the **Template** button in the application rules window and select a rule template from the context menu.

   Allow all is a rule that allows any network activity for an application. **Block all** is a rule that blocks any network activity for an application. All attempts to initiate a network connection by the application for which the rule has been created, will be blocked without notifying the user.

   Other templates listed on the context menu create a set of rules typical of the corresponding programs. For example, the **Mail Client** template creates a set of rules that allow standard network activity for mail clients, such as sending mail.

7. Edit the rules you have created, if necessary. You can edit the action, direction of the network connection, address, ports (local and remote), and time range for the rule.

   If you want the rule to apply to an application opened with certain settings in the command line, check the ☑ **Command line** box and enter the string in the field to the right.

   The rule (set of rules) created will be added to the end of the list with the lowest ranking priority. You can increase the priority ranking of the rule.

RULES FOR PACKET FILTERING. CREATING A RULE

Kaspersky Anti-Virus installation package includes a set of rules which determine the way of filtering data packets coming to and going from your computer. You can initiate data packet transfer on your own, or leave it to an application installed on your computer. Kaspersky Anti-Virus installation package includes rules for packet filtering applicable to packets whose transmission was thoroughly analyzed by Kaspersky Lab and was strictly defined as dangerous or safe.

Depending on the protection level selected for Firewall, and on the type of network the computer is running on, the list of rules can be used in various ways. Thus, for example, at the **High Security** level, all network activity not covered by allowing rules, is blocked.

Note that rules for security zones have higher priority than blocking packet rules. Thus, for example, if you select the **Local network** status, packet exchange will be allowed, and so will access to shared folders regardless of blocking packet rules.

➧ *To create a new packet rule:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.
5. In the window that will open, on the **Rules for packet filtering** tab, click the **Add** button.
6. The **New rule** window that will open provides a rule creation form that you can use to fine-tune a rule.

CHANGING RULE PRIORITY

A certain priority is set for each rule created for an application or for a packet. Other things being equal (such as the network connection settings), the action applied to an application's activity will be the rule with the highest priority.

The priority of a rule is determined by its position on the list of rules. The first rule on the list has the highest execution priority. Each rule created manually is added to the beginning of the list. Rules created using a template or from a special notification are added to the end of the list of rules.

➧ *To change an application rule's priority, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.
5. In the window that will open, on the **Rules for applications** tab, select an application name from the list and click the **Edit** button.
6. In the created rules window that will open, use the **Move up** and **Move down** buttons to move the rules inside the list, thus changing their priority.

➧ *To change the rule priority, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.
5. In the window that will open, on the **Rules for packet filtering** tab, select a rule. Use the **Move up** and **Move down** buttons to move the rule inside the list, thus changing its priority.

EXPORTING AND IMPORTING THE CREATED RULES

Export and import are designed to carry over the created rules to other computers. This helps to configure Anti-Hacker quickly.

➡ *To copy the created rules for application, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.
5. In the window that will open, on the **Rules for applications** tab, use the **Export** and **Import** buttons to perform the required actions on copying the rules.

➡ *To copy the created rules for packet filtering, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.
5. In the window that will open, on the **Rules for packet filtering** tab, use the **Export** and **Import** buttons to perform the required actions on copying the rules.

FINE-TUNING RULES FOR APPLICATIONS AND PACKET FILTERING

The fine tuning of rules being created and changed, is performed in accordance with the following procedure:

- Specifying a name for the rule. By default, the application uses a standard name that you can change.
- Selecting network connection settings which determine the rule's application: remote IP address, remote port, local IP address, local port, and duration of the rule.
- Modifying other settings that are responsible for informing the user that the rule has been applied.
- Assigning values for rule parameters and selecting actions. The action of every created rule is *allow*. To change it to a blocking rule, left-click on the **Allow** link in the rule description section. It will change to **Block**.
- Defining the direction of network connection (see section "Changing the direction of a network connection" on page 91) for the rule. The default value is a rule for both inbound and outbound network connection.
- Defining the protocol of network connection. TCP is the default protocol for the connection. If you are creating a rule for applications, you can select one of two protocols, TCP or UDP. If you create a rule for a packet, you can change the protocol type (see section "Changing data transfer protocol" on page 91). When selecting ICMP, you may need to further indicate the type (see section "Changing your ICMP packet type" on page 93).
- Specifying the fine-tuned settings of network connection (address (see section "Defining the network connection address" on page 92), port (see section "Defining the connection port" on page 92), time range (see section "Defining the time range of rule's activity" on page 92)), if they have been already selected.
- Ranking rule priority (see section "Changing the rule priority" on page 89).

You can create a rule from the network activity detection alert window.

The **New rule** window has a form that you can use to create a rule (for applications (see page 87), for packet filtering (see page 88)).

SEE ALSO

CHANGING DATA TRANSFER PROTOCOL

One of the properties for rules for applications and packet filtering is the data transfer protocol of network connection. TCP is used for both applications and packets by default when creating a rule.

➧ *To change the data transfer protocol, please do the following:*

1. In the **New rule** window (for applications (see page 87), for packet filtering (see page 88)) in the **Rule description** section, click the link with the name of the protocol.
2. In the **Protocol** window that will open, select the required value.

CHANGING THE DIRECTION OF CONNECTION

One of the properties for rules for applications and packet filtering is the direction of network connection.

If it is important for you to specifically set the direction of packets in the rule, select whether they are inbound or outbound packets. If you want to create a rule for data stream, select stream type: inbound, outbound, or both.

The difference between *stream direction* and *packet direction* is that when you create a rule for a stream, you define in which direction the connection is opened. The direction of packets when transferring data via this connection is not taken into consideration.

For example, if you configure a rule for data exchange with an FTP server that is running in passive mode, you should allow the outbound stream. To exchange data with an FTP server in active mode, you should allow both outbound and inbound streams.

➧ *To change data stream direction, please do the following:*

1. In the **New rule** window (for applications (see page 87), for packet filtering (see page 88)), in the **Rule description** section, click the link with the direction of the connection.
2. In the **Select direction** window that will open, select the required value.

DEFINING THE NETWORK CONNECTION ADDRESS

If you have selected a remote or local IP address of network connection as a rule setting, you should assign it the value which will determine the rule application.

To specify the network connection address, please do the following:

1. In the **New rule** window (for applications (see page 87), for packet filtering (see page 88)), in the **Properties** section, check the ☑ **Remote IP address** (or **Local IP address**) box. Then click the **Enter IP address** link in the **Rule description** section.

2. In the **IP address** window that will open, select the type of IP address and enter a value for it.

DEFINING THE CONNECTION PORT

When configuring rules, you can assign values to remote or local ports.

- *Remote port* is a port of a remote computer for connection.

- *Local port* is a port on your computer.

Local and remote ports for data transfer are correctly defined when a rule is being created directly from a notification of suspicious activity. This information is recorded automatically.

➡ *To specify the port while configuring rules, please do the following:*

1. In the **New rule** (for applications (see page 87), for packet filtering (see page 88)) window, in the **Properties** section, check the ☑ **Remote port** (or **Local port**) box. Then click the **Enter port** link in the **Rule description** section.

2. In the **Port** window that will open, enter a value for a port or for a range of ports.

DEFINING THE TIME RANGE OF RULE'S ACTIVITY

You can assign each rule a time range over the course of the day for it to operate in. For example, you can block ICQ from 9:30 am till 6:30 pm.

➡ *To set the rule application time, please do the following:*

1. In the **New rule** (for applications (see page 87), for packet filtering (see page 88)) window, in the **Properties** section, check the ☑**Time range** box. Then click the **specify the time range** link in the **Rule description** section.

2. In the **Time range** window that will open, in the **from** and **till** fields, set the time range for the rule.

DETERMINING SOCKET TYPE

The socket type that supports data transfer via certain protocol(s) may be defined for each rule.

➡ *To change the socket type, please do the following:*

1. In the **New rule** (for applications (see page 87)) window, in the **Properties** section, check the ☑ **Socket type** box. Then click the link with the name of the installed socket type in the **Rule description** section.

2. In the **Socket type** window that will open, select the required value for the setting.

CHANGING ICMP PACKET TYPE

ICMP (Internet Control Message Protocol) is designed to inform the packet sender of errors or complicated situations that occur during data transfer.

If you select ICMP as the data transfer protocol in a packet filtration rule that you create, you can also specify the type of ICMP message.

For example, using the Ping utility that sends certain ICMP queries and receives replies to them, a hacker could learn whether your computer is on or not. The application installation package includes a rule that blocks ICMP queries and replies to them, which in turn prevents potential attacks on your computer.

➨ *To change the type of ICMP packet, please do the following:*

1. In the **New rule** (for packets (see page 88)) window, in the **Properties** section, check the ☑ **ICMP type** box. Then click the link with the name of the ICMP packet type in the **Rule description** section.

2. In the **ICMP packet type** window that will open, select the required value.

RULES FOR SECURITY ZONES

After you install the application, Anti-Hacker analyzes your computer's network environment. Based on the analysis, the entire network space is broken down into conventional zones:

- *Internet* – the World Wide Web. In this zone, Kaspersky Anti-Virus operates as a personal firewall. At that, default rules for packets and applications regulate all network activity to ensure maximum security. You cannot edit protection settings when working in this zone, other than enabling Stealth Mode on your computer for added safety.

- *Security zones* – certain conventional zones that mostly correspond with subnetworks that your computer is added in (these could be local subnetworks at home or in office). By default, these zones are considered as average-risk zones when working in them. You can change the statuses of these zones based on how much you trust a certain subnetwork, and you can configure rules for packet filtering and applications.

If Anti-Hacker Training Mode is enabled, a window will open every time your computer connects to a new zone, displaying a brief description of it. You should assign a status to the zone, and network activity will be allowed based on that status:

- **Internet**. This is the default status assigned to the Internet, since when you are on it, your computer is subjected to all types of potential threats. It is recommended to select this status for networks not protected by any anti-virus applications, firewalls, filters etc. When you select this status, the application ensures maximum security for this zone:

  - blocking any network NetBIOS activity within the subnetwork;

  - blocking rules for applications and packet filtering that allow NetBIOS activity within this subnetwork.

  Even if you have created a shared folder, the information in it will not be available to users from subnetwork with this status. Additionally, if this status is selected for a certain subnetwork, you will not be able to access files and printers on other computers of this subnetwork.

- **Local network**. The application assigns this status to the majority of security zones detected when analyzing the computer's network environment, except for the Internet. This status is recommended for zones with an average risk factor (for example, corporate LANs). If you select this status, the application allows the following:

  - any network NetBIOS activity within the subnetwork;

  - applying rules for applications and packet filtering that allow NetBIOS activity within this subnetwork.

  Select this status if you want to grant access to certain folders or printers on your computer but block any other external activity.

- **Trusted**. It is only recommended to apply this status to zones that in your opinion are absolutely safe where your computer is not subject to attacks and attempts to gain access to your data. If you select this status, all network activity will be allowed. Even if the **High Security** level is selected and the blocking rules are created, they will not apply to remote computers from a trusted zone.

> Note that any restrictions or access to files is only in effect within this subnetwork.

You can use Stealth Mode for added security when using networks labeled **Internet**. This mode only allows network activity initiated from your computer. This actually means that your computer becomes invisible to its surroundings. This mode does not affect your computer's performance on the Internet.

> It is not recommended to use the Stealth Mode if the computer is being used as a server (for example, mail server or HTTP server). Otherwise, the computers that connect to the server will not see it in the network.

SEE ALSO

ADDING NEW SECURITY ZONES

The list of zones that your computer is registered on is displayed on the **Zones** tab. Each of them is assigned a status, provided a brief description of the network, and an indication if the Stealth Mode is used.

➧ *To add a new zone to the list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Firewall** section, click the **Settings** button.
5. In the window that will open, on the **Zones** tab, use the **Refresh** button. Anti-Hacker will search for potential zones for registration, and if any are detected, the application will ask you to select a status for them. Besides, you can add new zones to the list manually (for example, if you connect your laptop to a new network). To do so, use the **Add** button and fill in the necessary information in the **Zone settings** window that will open.

   To delete the network from the list, click the **Delete** button.

CHANGING SECURITY ZONE'S STATUS

When new zones are automatically added, address and subnet mask are automatically determined by the application. The program assigns each zone added the default **Local network** status. You can change it.

➧ *To change the security zone status, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.

4. In the window that will open, in the **Firewall** section, click the **Settings** button.

5. In the window that will open, on the **Zones** tab, select a zone from the list and use the appropriate link from the **Rule description** section below the list. You can perform similar actions as well as edit addresses and subnetwork masks in the **Zone settings** window which you can open with the **Edit** button.

ENABLING/DISABLING STEALTH MODE

You can also enable the Stealth Mode when using zones labeled **Internet**.

➧ *To enable the Stealth Mode, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the Settings item from the **Anti-Hacker** component context menu.

4. In the window that will open, in the **Firewall** section, click the **Settings** button.

5. In the window that will open, on the **Zones** tab, select a zone from the list and use the appropriate link from the **Rule description** section below the list.

CHANGING THE FIREWALL MODE

The Firewall mode controls Anti-Hacker's compatibility with applications that establish multiple network connections, as well as with network games.

- **Maximum compatibility** – Firewall ensures that Anti-Hacker will work optimally with applications that establish multiple network connections (file-sharing network clients). This mode may lead to slow reaction time in network applications since allowing rules have higher priority than stealth mode (stealth mode allows only the network activity initiated from your computer). If you encounter such problems, it is recommended that you use the **Maximum speed** mode.

- **Maximum speed** – Firewall ensures the best possible reaction time of network applications. However, in this mode a user may encounter connection problems in some network applications, since in Stealth Mode all inbound and outbound connections are blocked regardless of the rules created. To solve the problem, disable Stealth Mode.

Changes to the Firewall mode will not take effect until Anti-Hacker has been restarted.

➧ *To change the preset Firewall operation mode, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Anti-Hacker** component context menu.

4. In the window that will open, in the **Firewall** section, click the **Settings** button.

5. In the window that will open, on the **Additional** tab, in the **Firewall Mode** section, select the required mode.

INTRUSION DETECTION SYSTEM

All currently known network attacks that could endanger a computer are listed in the application databases. The Anti-Hacker **Intrusion Detection System** operates on a list of these attacks. The list of attacks that the module can detect is updated in the process of database updating (see section "Updating the application" on page 131). By default, Kaspersky Anti-Virus does not update attack databases.

Intrusion Detection System tracks network activity typical of network attacks and if it detects an attempt to attack your computer, it blocks all network activity of that computer involving your computer for one hour. A warning will appear on the screen stating that a network attack attempt has taken place, with specific information about the computer which attacked you. You can pause or disable the Intrusion Detection System.

➧ *To disable the Intrusion Detection System, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, uncheck the ☑ **Enable Intrusion Detection System** box.

   To stop the module without opening the application's settings window, select the **Stop** item from the component's context menu.

➧ *To block the attacking computer for a while, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Hacker** component context menu.
4. In the window that will open, in the **Intrusion Detection System** section, check the ☑ **Block the attacking computer for ... min.** box and type the time span (in minutes) in the field.

NETWORK MONITOR

You can see the detailed information about all the connections established on your computer, open ports, and the volume of inbound and outbound traffic. To do so, use the **Network Monitor** command from the context menu.

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

- *Established connections* – the tab displays all network connections currently active on your computer. This includes both connections initialized by your computer and inbound connections.
- *Open ports* – the tab lists all open ports on your computer.
- *Traffic* – the tab displays the volume of information received and sent between your computer and other computers on the network that you are currently work on.

TYPES OF NETWORK ATTACKS

There are currently a multitude of various network attacks that exploit vulnerabilities in operating systems and other software, whether system-type or application-type, installed on your computer. Malefactors constantly develop attack methods, learning how to steal confidential information, make the system malfunction, or take total control over your computer to use it as part of a zombie network for perpetrating new attacks.

To ensure the security of your computer, you should know what kinds of network attacks you might encounter. Known network attacks can be divided into three major groups:

- **Port scan** – this threat type is not an attack itself, but it usually precedes one, since it is one of the common ways of obtaining information about a remote computer. The UDP/TCP ports used by the network tools on the targeted computer are scanned to find out their status (closed or open).

  Port scans can tell a hacker what types of attacks will work on that system, and what types will not. In addition, the information obtained by the scan (a model of the system) will help the malefactor to know what operating system the remote computer uses. This, in turn, further restricts the number of potential attacks, and, correspondingly, the time spent perpetrating them. It also aids a hacker in attempting to use vulnerabilities characteristic of the operating system.

- **DoS attacks, or Denial of Service attacks** are attacks, which cause an unstable functioning of a system or its crash. The consequences of these attacks can be damage or corruption of the information resources that they target and the inability to use those resources.

  There are two basic types of DoS attacks:

  - sending the target computer specially created packets that the computer does not expect, which causes the system to restart or stop;

  - sending the target computer many packets within a timeframe that the computer cannot process, which cause system resources to be exhausted.

  The following attacks are common examples from this group:

  - The *Ping of death attack* consists in sending an ICMP packet with a size greater than the maximum of 64 KB. This attack can crash some operating systems.

  - *Land attack* consists in sending a request to an open port on the target computer to establish a connection with itself. This sends the computer into a cycle, which intensifies the load on the processor and can lead to crashing of some operating systems.

  - The *ICMP Flood attack* consists in sending a large quantity of ICMP packets to your computer. The computer attempts to reply to each inbound packet, which slows the processor to a crawl.

  - The *SYN Flood attack* consists in sending a large quantity of queries to a remote computer to establish a fake connection. The system reserves certain resources for each of those connections, which completely drains your system resources, and the computer stops reacting to other connection attempts.

- **Intrusion attacks**, which aim to take over your computer. This is the most dangerous type of attack, since if it is successful, the hacker has complete control of your computer.

  Hackers use this attack to obtain confidential information from a remote computer (for example, credit card numbers, passwords), or to penetrate the system to use its computing resources for malicious purposes later (e.g., to use the invaded system in a zombie network, or as a platform for new attacks).

  This group is the largest by the number of attacks included. They may be divided into three groups depending on the operating system: Microsoft Windows attacks, Unix attacks, and the common group for network services available in both operating systems.

  The following types of attacks are the most wide-spread among those using the network resources of operating systems:

  - *Buffer overflow attacks* is a type of software vulnerability caused by a lack (or deficiency) of control when working with data arrays. This is one of the oldest vulnerability types and the easiest for hackers to exploit.

  - *Format string attacks* is a type of software vulnerability that arises from insufficient control of input values for I/O functions such as printf(), fprintf(), scanf(), and others, from the C standard library. If a program has this vulnerability, the hacker, with the ability to send queries created with a special technique, can gain complete control or the system.

Intrusion Detection System (see page 96) automatically analyzes and prevents attempts to exploit these vulnerabilities in the most common network services (FTP, POP3, IMAP) if they are running on the user's computer.

Microsoft Windows attacks are based on taking advantage of vulnerabilities in the software installed on the computer (for example, programs as Microsoft SQL Server, Microsoft Internet Explorer, Messenger, and system components that can be accessed via the network – DCom, SMB, Wins, LSASS, IIS5).

For example, Anti-Hacker protects your computer from attacks that use the following known software vulnerabilities (this list of vulnerabilities is cited with the Microsoft Knowledge Base numbering system):

(MS03-026) DCOM RPC Vulnerability(Lovesan worm)

(MS03-043) Microsoft Messenger Service Buffer Overrun

(MS03-051) Microsoft Frontpage 2000 Server Extensions Buffer Overflow

(MS04-007) Microsoft Windows ASN.1 Vulnerability

(MS04-031) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(MS04-032) Microsoft Windows XP Metafile (.emf) Heap Overflow

(MS05-011) Microsoft Windows SMB Client Transaction Response Handling

(MS05-017) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(MS05-039) Microsoft Windows Plug-and-Play Service Remote Overflow

(MS04-045) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(MS05-051) Microsoft Windows Distributed Transaction Coordinator Memory Modification

In addition, there are isolated incidents of intrusion attacks using various malicious scripts, includes scripts processed by Microsoft Internet Explorer and Helkern-type worms. The essence of this attack type consists in sending a special type of UDP packets to a remote computer that can execute malicious code.

Remember that, while on the network, your computer is at risk of being attacked by a hacker every day. To ensure your computer's security, be sure to enable the Anti-Hacker component when surfing the Internet, and update the network attack databases regularly (see section "Selecting objects to update" on page 136).

ANTI-HACKER STATISTICS

All operations of Anti-Hacker are logged in a report. The information about the component functioning is grouped on the tabs:

- *Network attacks* – this tab displays the list of all network attacks which have been attempted during the current Kaspersky Anti-Virus session.
- *Banned hosts* – this tab displays the list of all hosts blocked due to various reasons, for example, attempted attack on your computer, or if they were blocked by a rule.
- *Application activity* – this tab displays the activity of the applications on your computer.
- *Packet filtering* – this tab lists all data packets filtered according to a Firewall rule.
- *Settings* – on this tab you can find the settings ruling the functioning of Anti-Hacker.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **Anti-Hacker** component context menu.

ANTI-SPAM

Kaspersky Anti-Virus comprises *Anti-Spam*, the component that allows detecting unwanted messages (spam) and processing them in accordance with the rules in your email client saving time while working with the mail.

Anti-Spam uses a self-training algorithm (see section "Component operation algorithm" on page 101), which allows the component over time to distinguish between spam and "good" mail more accurately. The source of data for the algorithm is the contents of the message. To differentiate spam and good mail efficiently, Anti-Spam should be trained (see section "Training Anti-Spam" on page 102).

Anti-Spam is built into the following mail clients as a plug-in:

- Microsoft Office Outlook.
- Microsoft Outlook Express (Windows Mail).
- The Bat!

By creating a white or a black list of addresses you can let Anti-Spam know messages from which addresses it should consider "good" messages and messages from which addresses it should consider spam. Additionally, Anti-Spam can analyze messages for the presence of phrases from the lists of allowed and banned phrases.

Anti-Spam allows you to view mail on the server and delete unwanted messages without downloading them to your computer.

➡ *To edit Anti-Spam settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

COMPONENT OPERATION ALGORITHM

Anti-Spam's operation consists of two stages:

- First, Anti-Spam applies rigid filtering criteria to the message. Those criteria allow a quick determination as to whether the message is spam or not. Anti-Spam assigns the message the *spam* or *not spam* status, the scan will be stopped, and the message will be transferred to the mail client for processing (see Steps 1 through 5 below).
- At the further steps of the algorithm (see Steps 6 through 10 below), Anti-Spam analyzes email messages that have passed precise selection criteria at the previous steps. Such messages cannot be unambiguously considered spam. Therefore Anti-Spam has to calculate the *probability* of this message being spam.

Provided below is a more detailed discussion of the Anti-Spam operation algorithm:

1. The sender's address is scanned for matches on black and white lists of addresses:
   - if a sender's address is in the list of allowed senders, the message will be assigned the *not spam* status;
   - if a sender's address is in the list of blocked senders, the message will be assigned the *spam* status.

2. If a message was sent using Microsoft Exchange Server and scanning of such messages is disabled, the message will be assigned the *not spam* status.

3. The message is subject to the analysis for lines from the list of allowed phrases. If at least one line from this list has been found, the message will be assigned the *not spam* status.

4. The message is subject to the analysis for lines from the list of banned phrases. Detection of words from this list in the message increases the chances of the messages being spam. When the calculated probability is over 100%, a message will be assigned the *spam* status.

5. If message text contains an address included into the database of suspicious and phishing web addresses, the message receives the *spam* status.

6. The application analyzes the email message using the PDB technology. While doing it, Anti-Spam compares the headers of mail messages with the samples of headers of spam messages. Each match increases the probability that the message is in fact spam.

7. The application analyzes the email message using the GSG technology. While doing it, Anti-Spam analyzes images attached to the email message. If the analysis reveals signs typical of spam in the objects attached to the message, the probability of it being spam increases.

8. Anti-Spam analyzes email message using Recent Terms technology. While doing it, Anti-Spam searches for phrases characteristic of spam in the text. These phrases are contained in the updatable Anti-Spam databases. After the analysis is complete, Anti-Spam calculates how much the probability of the message being spam has increased.

9. It checks for the presence of the additional features (see section "Using additional spam filtering features" on page 109), typical of spam. Each detected feature increases the probability that the message being scanned is in fact spam.

10. If Anti-Spam has been trained, the message will be scanned using the iBayes technology. The self-training iBayes algorithm calculates the probability that the message is spam, based on the frequency of occurrence of phrases characteristic of spam in the text.

The result of the message analysis is the **probability** that the email message is spam. Spam creators constantly improve spam camouflage, therefore the calculated probability does not reach 100% in most cases. To ensure efficient filtering of the email message stream, Anti-Spam uses two parameters:

- *Spam rating* – probability value, which will cause the message to be considered spam when exceeded. If the probability is below this threshold value, the message is assigned the *potential spam* status.

- *Potential spam rating* – probability value, which will cause the message to be considered potential spam when exceeded. If the probability is less than this value, Anti-Spam will consider the message not spam.

Depending on the specified spam and potential spam ratings, messages will be assigned the *spam* or *potential spam* status. Messages will be also assigned the **[!! SPAM]** or **[!! Probable Spam]** label in the **Subject** field. Then they are processed according to the rules (see section "Actions on spam" on page 113) you have created for your mail client.

SEE ALSO

Anti-Spam...100

TRAINING ANTI-SPAM

One of the most powerful spam detection tools is the self-training iBayes algorithm. This algorithm makes a decision about the message's status based on the phrases it includes. Before starting, sample strings of useful and spam mail should be submitted to the iBayes algorithm to train it.

There are several approaches to Anti-Spam training:

- Using the Training Wizard (see section "Training using the Training Wizard" on page 103) (packet training), preferable from the very onset of using Anti-Spam.
- Training Anti-Spam using outgoing messages (see section "Training using outgoing email messages" on page 104).
- Training directly while working with email (see section "Training using Email client" on page 104) using special buttons on the mail client toolbar or menu items.
- Training when working with Anti-Spam reports (see section "Training with reports" on page 105).

SEE ALSO

TRAINING USING THE TRAINING WIZARD

The Training Wizard can train Anti-Spam (packet training) by indicating which mailbox folders contain spam and good mail.

Correct spam recognition requires training using at least 50 useful messages and 50 samples of unwanted mail. If you do not, the iBayes algorithm will not work.

To save time, the Training Wizard only trains on 50 emails in each selected folder.

This wizard consists of a series of boxes (steps) navigated using the **Back** and **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To stop the wizard at any step, use the **Cancel** button.

➧ *To start the Training Wizard, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Training** section, click the **Training Wizard** button.

When performing training based on good email messages, addresses of the message senders will be added to the list of allowed senders.

➧ *To disable adding the sender's address to the white list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, click the **Customize** button in the Sensitivity section.

5. In the window that will open, on the **White list** tab, in the **Allowed senders** section, uncheck the ☑ **Add allowed senders addresses when training Anti-Spam in the mail client** box.

TRAINING USING OUTGOING EMAIL MESSAGES

You can train Anti-Spam using a sample of 50 outgoing emails. The receivers' addresses will automatically be added to the white list.

➧ *To train Anti-Spam on outgoing emails:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **General** tab, in the **Outgoing mail** section, check the ☑ **Train on outgoing mail** box.

➧ *To disable adding the sender's address to the white list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, click the **Customize** button in the Sensitivity section.
5. In the window that will open, on the **White list** tab, in the **Allowed senders** section, uncheck the ☑ **Add allowed senders addresses when training Anti-Spam in the mail client** box.

TRAINING USING EMAIL CLIENT

Training while working directly with email involves using special buttons on your mail client's toolbar.

➧ *To train Anti-Spam using the email client, please do the following:*

1. Start the email client.
2. Select a message you wish to use for Anti-Spam training.
3. Perform one of the following actions depending on the email client you are using:
   - click the **Spam** or **Not Spam** button in the Microsoft Office Outlook toolbar;
   - click the **Spam** or **Not Spam** button in the Microsoft Outlook Express toolbar (Windows Mail);
   - use the special **Mark as Spam** and **Mark as Not Spam** items in the **Special** menu of The Bat! email client.

Anti-Spam will perform training using the selected message. If you select several emails, training will take place on all of them.

When you mark a message as non-spam, the address of the message sender is added to the list of allowed senders.

➡ *To disable adding the sender's address to the white list, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the White list tab, in the **Allowed senders** section, uncheck the ☑ **Add allowed senders addresses when training Anti-Spam in the mail client** box.

If you need to select several emails at once, or are certain that a folder contains emails of a single group (spam or not spam), you can take a multi-faceted approach to training using the Training Wizard.

Training with reports

You have the option of training Anti-Spam based on reports. The component's reports can help you assess the accuracy of the component's configuration, and if necessary, make certain corrections to Anti-Spam.

➡ *To mark a certain message as spam or not spam, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **Anti-Spam** component context menu.
4. In the window that will open, on the **Events** tab, select the message you want to use as a basis for additional training.
5. Select one of the following actions from the context menu for the message:
   - **Mark as Spam**.
   - **Mark as Not Spam**.
   - **Add to White list**.
   - **Add to Black list**.

Changing the Sensitivity Level

Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 protects you from spam at one of the following levels:

- **Block all** – the highest severity level where any email is considered as spam except for messages, which contain lines from the white list of phrases, and the senders of which are included in the white list of addresses. All other features are disabled.
- **High** – a high level that, when activated, raises the likelihood that some emails that are not actually spam, will be marked as *spam*. At this level, the message is analyzed using the white and black lists of addresses and phrases, and also using PDB, GSG technologies and iBayes algorithm.

  This level should be applied in cases when there is a high likelihood that the recipient's address is ignored by spammers. For example, when the recipient is not registered in the mass mailings and does not have an email address on free/non-corporate mail servers.

- **Recommended** – the most universal settings level for classifying email messages.

  At this level, it is possible that some spam will not be detected. This shows that Anti-Spam is not trained well enough. We recommend that you conduct an additional training for the module using the Training Wizard or the **Spam** / **Not Spam** buttons (menu items in the Bat!), using the spam letters that were not detected.

- **Low** – more loyal settings level. It could be recommended for users whose incoming correspondence for some reason contains a significant number of words recognized by Anti-Spam as spam, but is not. The cause of such a situation may be the professional activity of the recipient, by virtue of which he is forced to use professional terms in his correspondence with colleagues that are widespread in spam. All spam detection technologies are used to analyze emails at this level.

- **Allow all** – the lowest sensitivity level where only email messages, which contain lines from the black list of phrases, and the senders of which are included in the black list of addresses, are considered as spam. All other features are disabled.

By default, the protection against spam is set at the **Recommended** sensitivity level. You can boost or reduce the level, or change the settings for the current level.

➧ *To change the selected Anti-Spam component sensitivity level, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, move the sliding bar along the scale of sensitivity level. By adjusting the sensitivity level, you define the correlation between spam, probable spam, and good mail factors.

FILTERING EMAIL MESSAGES AT THE SERVER. MAIL DISPATCHER

Mail Dispatcher is designed for viewing the list of email messages on the server without downloading them to your computer. The opportunity allows you to reject some messages saving time and traffic while working with email and also decreasing the risk of downloading spam or viruses to your computer.

Mail Dispatcher is used to manage the messages residing on the server. Mail Dispatcher window opens every time before mail retrieval provided it is enabled.

Mail Dispatcher opens only when mail is received via POP3 protocol. Mail Dispatcher does not appear if your POP3 server does not support viewing of email headers, or if all messages at the server are from the addresses included in the white list.

The list of email messages residing at the server is displayed in the central part of the Dispatcher window. Select the message on the list for a detailed analysis of its header. Header viewing may be useful, for example, in the situation described below. Spammers install a malicious program on your colleague's computer; this program sends spam with his or her name on it, using his or her mail client's contact list. The probability that your address is present in the contact list of your colleague is quite high. Certainly it will result in lots of spam sent to your mailbox. In such cases, you cannot determine if a message has been sent by your colleague, or by a spammer using the sender's address only. Use the email headers! Check carefully to see who sent the email, when, and what size it is. Trace the path of the email from the sender to your mail server. All this information should be contained in the email headers. Make a decision whether it is really necessary to download that email from the server, or if it is actually best to delete it.

➧ *To use Mail Dispatcher, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Anti-Spam** component context menu.

4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.

5. In the window that will open, on the **General** tab, check the ☑ **Open Mail Dispatcher when receiving email via POP3** box.

➡ *To delete messages from the server using Mail Dispatcher, please do the following:*

1. Check the boxes next to the message in the **Delete** column in the Dispatcher window.

2. Click the **Delete selected** button in the top part of the window.

Messages will be deleted from the server. You will receive a notification marked as **[!! SPAM]** and processed according to the rules set for your mail client.

EXCLUDING MICROSOFT EXCHANGE SERVER MESSAGES FROM THE SCAN

You can exclude email messages which originate within the internal network (for example, corporate mail), from anti-spam scan. Please note that messages will be considered as internal mail, if Microsoft Office Outlook is used on all network computers and user mailboxes are located on the same Exchange server or on servers linked via X400 connectors.

By default, Anti-Spam does not scan Microsoft Exchange Server messages.

➡ *If you wish Anti-Spam to analyze the messages, please do the following:*

1. Open the main application window.

2. In the left part of the window, select the **Protection** section.

3. Select the **Settings** item from the **Anti-Spam** component context menu.

4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.

5. In the window that will open, on the **General** tab, uncheck the ☑ **Do not check Microsoft Exchange Server native messages** box.

SELECTING THE SCAN METHOD

The scan methods mean checking links inside email messages to identify if they are included in the list of suspicious web addresses and / or in the list of phishing addresses.

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

A phishing attack can be disguised, for example, as a letter from your bank with a link to its official web site. By clicking the link, you go to an exact copy of the bank's website and can even see the real address in the browser, even though you are actually on a counterfeit site. From this point forward, all your actions on the site are tracked and can be used to steal your money.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **General** tab, check the ☑ **Check if URLs are listed in the base of suspicious web addresses** box.

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

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **General** tab, check the ☑ **Check if URLs are listed in the base of phishing web addresses** box.

SELECTING THE SPAM FILTERING TECHNOLOGY

Emails are scanned for spam by using state-of-the-art filtration technologies.

By default the program uses all filtering technologies, allowing the most complete analysis of email messages for spam.

➡ *To disable any of the filtration technologies:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **Algorithms** tab, in the **Recognition algorithms** section, uncheck the ☑ boxes for the filtering technologies you do not wish to use for spam analysis of email messages.

DEFINING SPAM AND POTENTIAL SPAM FACTORS

Specialists of Kaspersky Lab have done all their best to configure Anti-Spam optimally for it to detect spam and potential spam.

Spam detection operations based on state-of-the-art filtration technologies helps the user train Anti-Spam to recognize quite accurately spam, potential spam, and good mail with a certain number of emails from your inbox.

Anti-Spam is trained by working with the Training Wizard, and training from email clients. While doing so, every individual element of good emails or spam are assigned a factor. When an email message enters your inbox, Anti-Spam scans the message using the iBayes algorithm for elements of spam and of good email. The factors for each element are totaled, and the spam rating and potential spam rating are calculated.

The probable spam factor value defines a limit above which the email will be classified as probable spam. If you are using the **Recommended** Anti-Spam sensitivity level, any email with a factor value between 50% and 59% will be considered probable spam. Good mail refers to mail that, after being scanned, has a spam factor of less than 50%.

The spam factor value defines a limit above which the email will be classified as spam. Any message with rating value higher than the one specified, will be perceived as spam. By default, the spam rating is 59% for the **Recommended** level. This means that any message with the rating higher than 59% will be marked as spam.

➡ *To edit Anti-Spam settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **Algorithms** tab, adjust the spam and probable spam factors in appropriate sections.

USING ADDITIONAL SPAM FILTERING FEATURES

In addition to the main features used to filter spam (creating white and black lists, analysis with filtering technologies), you can set additional features. Based on these features, a message will be assigned the **spam** status with a certain degree of probability.

Spam could be empty emails (no subject or body), emails containing links to images or with embedded images, with text in a very small font size. Spam can also be emails with invisible characters (the text matching the background color), emails containing hidden elements (elements that are not displayed at all), or incorrect HTML tags, and emails containing scripts (a series of instructions executed when the user opens the email).

➡ *To configure additional spam filtering features, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **Algorithms** tab, click the **Additional** button.
6. In the **Additional** window that will open, check the boxes next to the selected spam signs. For the included additional features, specify the spam factor (using percentage) which would establish the probability of classifying a message as spam. The default value for the spam factor is 80%.

   The spam probability value calculated thanks to the use of additional spam filtering features is added to the general verdict returned to the entire message by Anti-Spam.

   If you enable filtering by the "increase spam factor for messages not sent specifically to me" feature, you should specify the list of your trusted email addresses. To do so, click the **My addresses** button. In the **My addresses** window that will open specify the list of addresses and address masks. When scanning a message, Anti-Spam also verifies the address of the recipient. If the address does not match any of those on your list, the email will be labeled as **spam**.

CREATING THE LIST OF ALLOWED SENDERS

The white list of addresses contains the addresses of message senders from whom, in your opinion, no spam can be received. The white list of addresses is filled automatically while you train the Anti-Spam component. You can edit it.

The list can contain either addresses or address masks. When entering an address mask, you can use the standard ***** and **?** wildcards where ***** represents any combination of characters and **?** stands for any single character. Examples of address masks:

- *ivanov@test.ru* – messages from this address will always be classified as good mail;
- **@test.ru* – mail from any sender from the test.ru mail domain will always be considered good mail; for example: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – the sender with this name, regardless of the mail domain, always sends only good mail; for example: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – mail from any sender from a mail domain, starting with *test*, are considered not spam; for example: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – emails from a sender, whose name starts with *ivan.*, and whose mail domain name starts with *test* and ends with any three characters, is always considered not spam; for example: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

➡ *To create the list of allowed senders, do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, on the **White list** tab, in the **Allowed senders** section, check the ☑ **Consider emails from the following senders as not spam** box, and click the **Add** button.
5. In the **Email address mask** window that will open, enter the required address or mask.

CREATING THE LIST OF ALLOWED PHRASES

The white list of allowed phrases contains key phrases of messages which you have marked as non-spam. You can create such a list.

You can also use masks for phrases. When creating a mask, you can use the standard ***** or **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character. Examples of phrases and phrase masks:

- *Hi, Ivan!* – an email message that contains this text only is a good email. The use of the lines similar to the following lines is not recommended.
- *Hi, Ivan!** – an email message beginning with the phrase *Hi, Ivan!* is good.
- *Hi, *! ** – emails beginning with the greeting *Hi* and an exclamation point anywhere in the email are not spam.
- ** Ivan? ** – emails beginning with *Ivan* personal address followed by any character, are not spam.
- ** Ivan\? ** – emails containing the phrase *Ivan?* are good.

If characters * and ? are included into a phrase, then they should be preceded by the \ character to prevent their misrecognition in Anti-Spam. Then two characters are used instead of one: * and \?.

➧ *To create the list of allowed phrases:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **White list** tab, in the **Allowed phrases** section, check the ☑ **Consider emails containing the following phrases as not spam** box and click the **Add** button.
6. In the **Allowed phrase** window that will open, enter a line or a mask.

IMPORT OF ALLOWED SENDERS LIST

Addresses in the white list can be imported from *.txt*, *.csv* files, or from Microsoft Office Outlook / Microsoft Outlook Express address book.

➧ *To import the list of allowed senders, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **White list** tab, in the **Allowed senders** section, click the **Import** button.
6. Select the import source from the dropdown menu:
   - If you have selected the **From file** item, the file selection window will open. The application supports import from *.csv* or *.txt* file types.
   - If you have selected the **From Address Book** item, the address book selection window will open. Select the required address book from this window.

CREATING THE LIST OF BLOCKED SENDERS

The black list contains the addresses of senders of messages which have been marked as spam. The list is filled manually.

The list can contain either addresses or address masks. When entering a mask, you can use the standard ***** and **?** wildcards, where ***** represents any combination of characters and **?** stands for any single character. Examples of address masks:

- *ivanov@test.ru* – messages from this address will always be classified as spam;
- **@test.ru* – mail from any sender from the *test.ru* mail domain will always be classified as spam; for example: *petrov@test.ru*, *sidorov@test.ru*;

- *ivanov@** – the sender with this name, regardless of the mail domain, always sends only spam; for example: *ivanov@test.ru*, *ivanov@mail.ru*;

- **@test** – mail from any sender from a mail domain, starting with *test*, are considered spam; for example: *ivanov@test.ru*, *petrov@test.com*;

- *ivan.*@test.???* – emails from a sender, whose name starts with *ivan.*, and whose mail domain name starts with *test* and ends with any three characters, is always considered not spam; for example: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

➡ *To create the list of blocked senders, do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.
5. In the window that will open, on the **Black list** tab, in the **Blocked senders** section, check the ☑ **Consider emails from the following senders as spam** box, and click the **Add** button.
6. In the **Email address mask** window that will open, enter the required address or mask.

CREATING THE LIST OF BANNED PHRASES

The black list of senders stores key phrases from emails that you regard as spam. The list is filled manually.

You can also use masks for phrases. When creating a mask, you can use the standard ***** or **?** wildcards, where ***** represents any combination of characters and ? stands for any single character. Examples of phrases and phrase masks:

- *Hi, Ivan!* – an email message that contains this text only is a spam. It is not recommended to use such a phrase as a listed phrase.

- *Hi, Ivan!** – an email beginning with the phrase *Hi, Ivan!* is spam.

- *Hi, *! ** – an email beginning with *Hi* and an exclamation mark in any part of the message is spam.

- ** Ivan? ** – an email contains a greeting to a user with the name *Ivan* whose name is followed by any character, and is spam.

- ** Ivan\? ** – an email message containing the *Ivan?* phrase is spam.

If characters * and ? are included into a phrase, then they should be preceded by the \ character to prevent their misrecognition in Anti-Spam. Then two characters are used instead of one: * and \?.

When scanning an email, Anti-Spam analyzes its content against strings from the black list. Detection of words from this list in the message increases the chances of the messages being spam. When the calculated probability is over 100%, a message will be assigned the *spam* status.

➡ *To create the list of blocked phrases:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.

4. In the window that will open, in the **Sensitivity** section, click the **Customize** button.

5. In the window that will open, on the **Black list** tab, in the **Blocked phrases** section, check the ☑ **Consider emails containing the following phrases as spam** box and click the **Add** button.

6. In the **Blocked phrase** window that will open, enter a line or a mask.

ACTIONS TO BE PERFORMED ON SPAM

If after scanning you find that an email is spam or probable spam, further operations of Anti-Spam depend on the status of the object and the action selected. By default, email messages considered *spam* or *probable spam*, are modified: in the **Subject** field of the message, the **[!! SPAM]** or **[?? Probable Spam]** label is added, respectively.

You can select additional actions to be taken on spam or probable spam. To do so, special plug-ins are provided in Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) and The Bat! clients. For other mail clients, you can configure the filtration rules.

SEE ALSO

CONFIGURING SPAM PROCESSING IN MICROSOFT OFFICE OUTLOOK

The spam processing settings window automatically opens the first time you run email client after installing the application.

By default, email messages classified by Anti-Spam as *spam* or *probable spam* are marked with the special **[!! SPAM]** or **[?? Probable Spam]** labels in the **Subject** field.

You can apply the following processing rules to both spam and probable spam:

- **Move to folder** – spam is moved to the folder of your inbox that you have specified.

- **Copy to folder** – a copy of the email message is created and moved to the specified folder. The original email is saved in your **Inbox**.

- **Delete** – delete spam from the user's mailbox.

- **Skip** – leave the email in the **Inbox** folder.

To do so, select the appropriate value from the dropdown list in the **Spam** or **Probable spam** section.

Additional actions on spam and probable spam in Microsoft Office Outlook can be found on the special **Anti-Spam** tab in the **Tools** → **Options** menu.

It opens automatically when the mail client is first opened after installing the application, and it asks if you want to configure spam processing.

When training Anti-Spam with mail client, a marked message will be sent to Kaspersky Lab as a spam sample. Click the **Additionally after manually marking emails as spam** link to select the spam sample transfer mode in the window that will open.

Also, you can select the algorithm for common operation of Microsoft Office Outlook and Anti-Spam plug-in:

- ● **Scan upon receiving**. All emails that enter the user’s inbox are initially processed according to the Microsoft Office Outlook rules. After processing is complete, the remaining messages that do not fall under any of the rules are processed by the Anti-Spam plug-in. In other words, emails are processed according to the priority of the rules. Sometimes the priority sequence may be ignored, if, for example, a large number of emails arrive in your inbox at the same time. As a result, situations could arise when information about an email processed by a Microsoft Office Outlook rule is logged in the Anti-Spam report marked with the *spam* status. To avoid this, we recommend configuring the Anti-Spam plug-in as a Microsoft Office Outlook rule.

- ● **Use Microsoft Office Outlook rule**. With this option, incoming messages are processed using the hierarchy of Microsoft Office Outlook rules, one of which should be a rule of processing emails by Anti-Spam. This is the best configuration, as it does not cause conflicts between Microsoft Outlook and the Anti-Spam plug-in. The only shortcoming of this arrangement is that you should create and delete spam processing rules through Microsoft Office Outlook manually.

➡ *To create a spam processing rule, please do the following:*

1. Run Microsoft Office Outlook and use the **Tools** → **Rules and Alerts** command in the main application menu. The command for opening the tool depends on your version of Microsoft Office Outlook. This Help file describes how to create a rule using Microsoft Office Outlook 2003.

2. In the **Rules and Alerts** window that will open, on the **Email Rules** tab, click the **New Rule** button. As a result, the Rules Wizard will be launched. Rules Wizard provides for the following steps:

   a. You should decide whether you want to create a rule from scratch or using a template. Select the **Start from a blank rule** option and select the **Check messages when they arrive** scan condition. Click the **Next** button.

   b. Click the **Next** button in the message filtering condition configuration window without checking any boxes. In the dialog box, confirm that you want to apply this rule to all emails received.

   c. In the window for selecting actions to apply to messages, check the ☑ **perform a custom action** box in the action list. In the bottom part of the window, click the **a custom action** link. Select **Kaspersky Anti-Spam** from the dropdown list in the window that will open, and click the **OK** button.

   d. Click the **Next** button in the exclusions from rules window without checking any boxes.

   e. In the final window, you can change the rule's name (the default name is **Kaspersky Anti-Spam**). Make sure that the ☑ **Turn on this rule** box is checked, and click the **Finish** button.

3. The default position for the new rule is first on the rule list in the **Rules and Alerts** window. If you like, move this rule to the end of the list so that it applies to the email last.

All incoming emails are processed with these rules. The order in which the rules apply to emails depends on the priority you assign to each rule. The rules apply from the beginning of the list. Each subsequent rule is ranked lower than the previous one. You can change the priority for applying rules to emails.

If you do not want the Anti-Spam rule to further process emails after a rule is applied, you should check the ☑ **Stop processing more rules** box in the rule settings (see Step 3 in creating a rule).

If you are experienced in creating email processing rules in Microsoft Outlook, you can create your own rule for Anti-Spam based on the algorithm that we have suggested.

SEE ALSO

Configuring spam processing in Microsoft Outlook Express (Windows Mail) 115

Configuring spam processing in The Bat! 115

CONFIGURING SPAM PROCESSING IN MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

The spam processing settings window opens when your run your client after the installation of the application.

By default, email messages classified by Anti-Spam as *spam* or *probable spam* are marked with the special **[!! SPAM]** or **[?? Probable Spam]** labels in the **Subject** field.

Additional actions on spam and probable spam in Microsoft Outlook Express (Windows Mail) can be found in a special window that opens when you click the **Settings** button near the other Anti-Spam buttons - **Spam** and **Not Spam** - on the taskbar.

It opens automatically when the mail client is first opened after installing the application and asks if you what to configure spam processing.

You can apply the following processing rules to both spam and probable spam:

- **Move to folder** – spam is moved to the folder of your inbox that you specify.
- **Copy to folder** – a copy of the email message is created and moved to the specified folder. The original email is saved in your **Inbox**.
- **Delete** – delete spam from the user's mailbox.
- **Skip** – leave the email in the **Inbox** folder.

To do so, select the appropriate value from the dropdown list in the **Spam** or **Probable spam** section.

When training Anti-Spam with mail client, a marked message will be sent to Kaspersky Lab as a spam sample. Click the **Additionally after manually marking emails as spam** link to select the spam sample transfer mode in the window that will open.

> Settings for spam processing are stored as Microsoft Outlook Express (Windows Mail) rules, therefore to save changes you should restart your Microsoft Outlook Express (Windows Mail).

SEE ALSO

Configuring spam processing in Microsoft Office Outlook 113

Configuring spam processing in The Bat! 115

CONFIGURING SPAM PROCESSING IN THE BAT!

Actions on spam and probable spam in The Bat! are defined by the client's own tools.

➧ *To set up spam processing rules in The Bat!, please do the following:*

1. Select the **Settings** item from the **Properties** menu of the mail client.
2. Select the **Spam protection** item from the settings tree.

Displayed settings of anti-spam protection apply to all installed Anti-Spam modules that support integration with The Bat!.

You should set the rating level, and specify how to respond to emails with a certain rating (in the case of Anti-Spam, the rating is the likelihood that the email is spam):

- delete the emails with a rating higher than a given value;
- move email messages with a given rating to a special spam folder;
- move spam marked with special headers to the spam folder;
- leave spam in the **Inbox** folder.

After processing an email, Kaspersky Anti-Virus assigns a spam or probable spam status to the message based on a rating with an adjustable value. The Bat! has its own email rating algorithm for spam, also based on a spam rating. For the spam factor values not to mismatch in Kaspersky Anti-Virus and in The Bat!, all messages scanned by Anti-Spam are assigned a rating, in accordance to the message status: good mail - 0%, probable spam - 50 %, spam - 100 %. Thus, the email rating in The Bat! corresponds to the rating of the corresponding status and not to the email rating assigned in Anti-Spam.

For more details on the spam rating and processing rules, see documentation for The Bat!.

SEE ALSO

RESTORING DEFAULT ANTI-SPAM SETTINGS

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

➡ *To restore default Anti-Spam settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Anti-Spam** component context menu.
4. In the window that will open, press the **Default level** button in the **Sensitivity** section.

ANTI-SPAM STATISTICS

General information about the component's functioning is saved in a special report where you can find a detailed report on the component's functioning grouped by several tabs:

- A complete list of events that have arisen while using the component is kept on the *Events* tab. This is where the results of the Anti-Spam training are displayed, showing the factor, category, and reasons for one or another email classification.

  Using the special context menu, you can train while viewing the report. To do so, select the name of the email, then open the context menu by right-clicking, and select **Mark as spam**, if the email is spam, or **Mark as not spam**, if the selected email is good mail. In addition, based on the information obtained by analyzing the email, you can enlarge the white and black lists of Anti-Spam. To do so, use the corresponding items on the context menu.

- The settings for email filtration and further processing are given on the *Settings* tab.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **Anti-Spam** component context menu.

ACCESS CONTROL

Access Control is a new component of Kaspersky Anti-Virus. It monitors users' access to the devices installed on the computer with the Device Control component. The component allows blocking applications' attempts to access certain types of external devices.

After Device Control is installed, it is disabled.

➡ *To enable Device Control, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Device Control** section.
3. In the right part of the window, check the ☑ **Enable Device Control** box.

➡ *To modify the Device Control settings, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Device Control** component context menu.
4. In the window that will open, make the required changes in the component settings.

IN THIS SECTION

DEVICE CONTROL. RESTRICTING THE USE OF EXTERNAL DEVICES

The Device Control module monitors interactions between applications and external devices installed on the computer.

By default, Device Control provides access to any device.

➡ *To restrict access of applications to devices, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Device Control** component context menu.
4. In the window that will open, click the **Settings** button.
5. In the **Settings: Device Control** window that will open, check the ☑ boxes for the types of devices you want to block.

To validate the changes, you should reconnect the device (for Firewire or USB devices), or reboot the computer (for other types of devices).

DEVICE CONTROL. DISABLE AUTORUN

You can block autorun by using the following options:

- Block autorun for all devices, which leads to disabling the AutoRun / AutoPlay functionality implemented in Microsoft Windows. This functionality allows reading data and automatically run programs from a removable medium connected to the computer.
- Block the processing of the autorun.inf file, which leads to blocking unauthorized attempts of running applications from removable media. This option allows blocking any operating system's attempts of executing potentially dangerous instructions in the autorun.inf file, without disabling the AutoPlay functionality completely.

The autorun is blocked by default. As hackers often use the autorun option to spread viruses via removable drives, Kaspersky Lab recommends you blocking it.

➡ *To block the autorun, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Settings** item from the **Device Control** component context menu.
4. In the window that will open, click the **Settings** button.
5. In the **Settings: Device Control** window that will open, in the **Autorun** section, check the corresponding ☑ boxes.

To validate the changes, you should reboot the computer.

ACCESS CONTROL STATISTICS

All operations performed by Device Control are logged in a special report where you can obtain detailed information on the component's operation grouped on tabs:

- All external devices blocked by the module are listed on the *Devices* tab.
- The *Settings* tab displays the settings, which regulate Access Control's operation.

➡ *To view information about the component's operation, please do the following:*

1. Open the main application window.
2. In the left part of the window, select the **Protection** section.
3. Select the **Report** item from the **Access Control** component context menu.

SCANNING COMPUTER FOR VIRUSES

Virus scan is one of the most important tools for protecting your computer. Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 can scan separate items (files, folders, disks, removable media) or the entire computer for viruses.

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

Scan

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

Full Scan

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

Quick Scan

Virus scan of operating system startup objects.

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

In addition, any object may be scanned (such as a hard drive storing software and games, email databases brought home from office, a compressed file received by email, etc.) without creating a dedicated scan task. An object to scan may be selected using the Kaspersky Anti-Virus interface or standard Microsoft Windows tools (for example, **Windows Explorer** or **Desktop**, etc.). Place the cursor on the desired object's name, right-click to open the Microsoft Windows context menu, and select the **Scan for viruses** option.

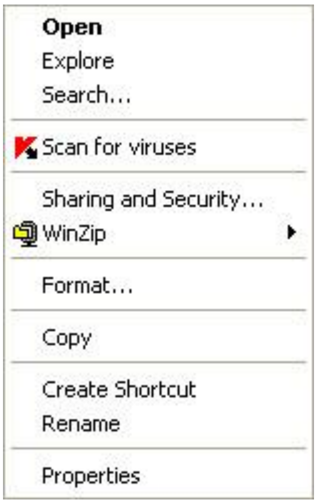


Figure 7. Microsoft Windows context menu

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

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

1. Open the main application window.
2. In the left part of the window, select the **Scan** (**Full Scan**, **Quick Scan**) section.
3. For the selected section, click the link with the preset security level.

4. In the window that will open, make the required changes in the settings of the task you have selected.

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

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

IN THIS SECTION

STARTING THE VIRUS SCAN

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

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

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

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

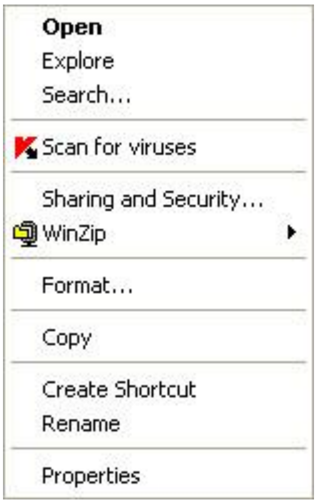


Figure 8. Microsoft Windows context menu

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

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

➧ *To start the virus scan task from the main application window:*

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

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

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

CREATING A LIST OF OBJECTS TO SCAN

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

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

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

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

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

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

CHANGING SECURITY LEVEL

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

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

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

➧ *To change the defined security level, perform the following actions:*

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

CHANGING ACTIONS TO BE PERFORMED ON DETECTED OBJECTS

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

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

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

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

IF THE ACTION SELECTED WAS	WHEN A MALICIOUS / POTENTIALLY INFECTED OBJECT IS DETECTED
● **Prompt for action when the scan is complete**	The application will postpone processing of objects until the scan is complete. When the scan is complete, the statistics window will pop up with a list of objects detected, and you will be asked if you want to process the objects.
● **Prompt for action during scan**	The application will display a warning message with information about which malicious code has infected or potentially infected the object, and will offer several options of further actions.
● **Do not prompt for action**	The application creates a report with information about objects detected without processing them or notifying the user. This application mode is not recommended, because it leaves infected or potentially infected objects on your computer making infection virtually inevitable.
● **Do not prompt for action** ☑ **Disinfect**	The application attempts to disinfect the object without requesting any confirmation from the user. If the attempt of disinfecting the object fails, it will be either blocked (if the object cannot be disinfected), or assigned the *potentially infected* status (if the object is considered suspicious), and it will be moved to Quarantine. Relevant information is logged in the report. Later you can attempt to disinfect this object.
● **Do not prompt for action** ☑ **Disinfect** ☑ **Delete if disinfection fails**	The application attempts to disinfect the object without requesting any confirmation from the user. If the object cannot be disinfected, it will be deleted.
● **Do not prompt for action** □ **Disinfect** ☑ **Delete**	The application deletes the object automatically.

Before attempting to disinfect or delete an infected object, Kaspersky Anti-Virus creates a backup copy of it, which is placed into Backup to allow later restoration or disinfection.

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

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

CHANGING THE TYPE OF OBJECTS TO SCAN

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

When selecting file types you should remember the following:

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

extension, the file protection will analyze the file header and may determine that the file is an .exe file. Such a file would be thoroughly scanned for viruses.

➡ *To change the type of scanned objects:*

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

SCAN OPTIMIZATION

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

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

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

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

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

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

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

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

5. In the window that will open, on the **Scope** tab, click the **Additional** button.

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

SCAN OF COMPOUND FILES

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

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

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

1. Open the main application window.

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

3. For the selected section, click the link with the preset security level.

4. In the window that will open, in the **Security Level** section, click the **Customize** button.

5. In the window that will open, on the **Scope** tab, in the **Scan of compound files** section, select the required type of compound files to be scanned.

SCAN TECHNOLOGY

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

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

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

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

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

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

1. Open the main application window.

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

3. For the selected section, click the link with the preset security level.

4. In the window that will open, in the **Security Level** section, click the **Customize** button.

5. In the window that will open, on the **Additional** tab, in the **Scan technologies** section, enable the required technology.

CHANGING THE SCAN METHOD

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

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

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

➧ *To specify which scan method to use:*

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

COMPUTER PERFORMANCE DURING TASK EXECUTION

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

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

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

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

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

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

RUN MODE: SPECIFYING AN ACCOUNT

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

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

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

RUN MODE: CREATING A SCHEDULE

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

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

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

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

➡ *To edit a schedule for scan tasks:*

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

➡ *To configure automatic launches of skipped tasks:*

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

FEATURES OF SCHEDULED TASK LAUNCH

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

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

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

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

VIRUS SCAN STATISTICS

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

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

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

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

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

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

ASSIGNING COMMON SCAN SETTINGS FOR ALL TASKS

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

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

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

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

RESTORING DEFAULT SCAN SETTINGS

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

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

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

UPDATING THE APPLICATION

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

Application update downloads and installs on your computer:

- **Application databases**

  The protection of information is based on databases which contain signatures of threats and network attacks, and the methods used to fight them. Protection components use these databases to search for dangerous objects on your computer and to disinfect them. The databases are added to every hour with records of new threats and methods used to fight them. Therefore, you are advised to update them on a regular basis.

  In addition to the application databases, the network drivers that enable the application's components to intercept network traffic are also updated.

- **Application modules**

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

Kaspersky Lab's update server is the primary source of updates for Kaspersky Anti-Virus.

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

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

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

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

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

You can also configure automatic update startup.

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

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

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

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.

4. In the window that will open, make the required changes in the settings of the task you have selected.

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

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

IN THIS SECTION

STARTING THE UPDATE

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

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

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

Update information will be displayed in the main application window.

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

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

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

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

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

ROLLING BACK THE LAST UPDATE

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

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

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

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

SELECTING AN UPDATE SOURCE

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

You can use the following as update sources:

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

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

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

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

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

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

➡ *To choose an update source:*

1. Open the main application window.
2. In the left part of the window, select the **Update** section.
3. For the selected section, click the link with the preset run mode.
4. In the window that will open, in the **Update settings** section, click the **Configure** button.
5. In the window that will open, on the **Update source** tab, click the **Add** button.
6. Select an FTP or HTTP site, or enter its IP address, symbolic name or URL in the **Select update source** window that will open.

REGIONAL SETTINGS

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

➡ *To choose the closest server:*

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

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

USING A PROXY SERVER

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

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

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

RUN MODE: SPECIFYING AN ACCOUNT

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

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

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

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

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

RUN MODE: CREATING A SCHEDULE

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

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

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

➧ *To edit a schedule for scan tasks:*

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

➧ *To configure automatic launches of skipped tasks:*

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

5. In the **Schedule** window that will open, in the **Schedule settings** section, check the ☑ **Run task if skipped** box.

CHANGING THE UPDATE TASK'S RUN MODE

You can select the run mode for Kaspersky Anti-Virus update task by using the application configuration wizard (see section "Configuring the update settings" on page 30). You can change the run mode you have selected.

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

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

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

- ◉ **On schedule** (time interval changes depending on settings). Updates will run automatically according to the schedule created.

- ◉ **Manually**. If you select this option, you will run application updates on your own. Kaspersky Anti-Virus will notify you when updates are required without fail.

➡ *To configure the update task launch schedule:*

1. Open the main application window.

2. In the left part of the window, select the **Update** section.

3. For the selected section, click the link with the preset run mode.

4. In the window that will open, select the update task launch mode in the **Run mode** section. If the scheduled update option is selected, create the schedule.

SELECTING OBJECTS TO UPDATE

Update objects are the components that will be updated:

- application databases;

- network drivers that enable protection components to intercept network traffic;

- network attack database used by Anti-Hacker;

- application modules.

Databases, network drivers, and the network attack database are always updated, and the application modules are only updated if they are configured properly.

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

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

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

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

UPDATING FROM A LOCAL FOLDER

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

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

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

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

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

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

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

UPDATE STATISTICS

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

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

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

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

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

POSSIBLE PROBLEMS DURING THE UPDATE

When you update Kaspersky Anti-Virus application modules or threat signatures, errors may occur, which is associated with incorrect update configuration, connection problems, etc. This Help section covers the major part of errors and gives tips for eliminating them. If you encounter errors not covered in Help or want detailed recommendations for eliminating them, try finding information in the Knowledge Base in the Technical Support web portal in the "If a program generated an error..." section. If recommendations given in this section are not helpful in solving the problem or if there is no information about the error in the Knowledge Base, send a request to the Technical Support Team.

Configuration errors

Errors of this group occur largely due to an incorrect installation of the application, or due to modifications of the application configuration, which resulted in a loss of functionality.

General recommendations:

If errors in this group are generated, we recommend restarting updates. If the error persists, contact Technical Support.

If the problem is connected to the application being installed incorrectly, we recommend reinstalling it.

No update source specified

None of the source contains update files. It is possible that no update source is specified in the update settings. Please make sure that the update settings are configured correctly and try again.

Error verifying license

This error is generated if the license key used by the application is blocked and placed in the license black list.

Error retrieving update settings

Internal error retrieving update task settings. Please make sure that update settings are configured correctly and try again.

Insufficient privileges to update

This error usually occurs when the user account used to start the update does not have access privileges to the update source. We recommend making sure that user account has the necessary privileges.

This error could also be generated when attempt to copy update files to a folder that cannot be created.

Internal error

Internal logical error in update task. Please make sure that the update settings are configured correctly and try again.

Error verifying updates

This error is generated if the files downloaded from the update source do not pass internal verification. Please try updating later.

Errors that occur when working with files and folders

This type of error occurs when the user account being used to run updates has restricted rights or no rights to access the update source or the folder where the updates are located.

General recommendations:

If errors of this type occur, we recommend verifying that the user account has sufficient access rights to those files and folders.

Cannot create folder

This error is generated if a folder cannot be created during the update procedure.

Insufficient privileges to execute file operation

This error occurs if the user account used to run the update does not have sufficient privileges to execute operations with the files.

File or folder not found

This error occurs if a file or folder needed in updates is missing. We recommend verifying that the specified file or folder exists and is available.

File operation error

This error is an internal logical error of the update module when executing operations with files.

NETWORK ERRORS

Errors of this group occur when there are connection problems or when network connection is not configured correctly.

General recommendations:

If errors in this group occur, we recommend making sure your computer is connected to the Internet, the connection settings are correctly configured, and the update source is available. Then try updating again. If the problem persists, contact Technical Support.

Network error

An error was generated while retrieving update files. If you encounter this error, check your computer's network connection.

Connection interrupted

This error occurs when the connection with the update source is terminated by the update server for any reason.

Network operation timeout

Update source connection timeout. When configuring the program's update settings, you may have set a low time-out value for the connection with the update source. If your computer cannot connect to the server or the update folder within that time, the program returns this error. In such a case, we recommend checking that the settings for Updater are correct and that the update source is available.

Authorization error on FTP server

This error occurs if authorization settings for the FTP server used as the update source are entered incorrectly. Please make sure that the actual FTP server settings allow this user account to download files.

Authorization error on proxy server

This error is generated if the settings for updating via a proxy server incorrectly indicate the name and password, or if the user account under which the updates are run does not have access privileges to the update source. Please, edit the authorization settings and retry the update.

Error resolving DNS name

This error is generated if no update source is detected. It is possible that the update source address is indicated incorrectly, the network settings are incorrect, or the DNS server is unavailable. We recommend checking your update settings and availability of update sources, then try again.

Connection to the update source could not be established

This error occurs is there is no connection with the update source. Please make sure that the update source settings are configured correctly and try again.

Connection to the proxy server could not be established

This error is generated if the proxy server connections settings are indicated incorrectly. To solve the problem, we recommend making sure that settings are configured correctly, the proxy server is available, and the Internet is available, and trying to update again.

Error resolving proxy server DNS name

This error is generated if the proxy server is not detected. We recommend making sure that the proxy server settings are correct and that the DNS server is available.

ERRORS RELATED TO CORRUPTED DATABASES

These errors are linked to corrupted files in the update source.

General recommendations:

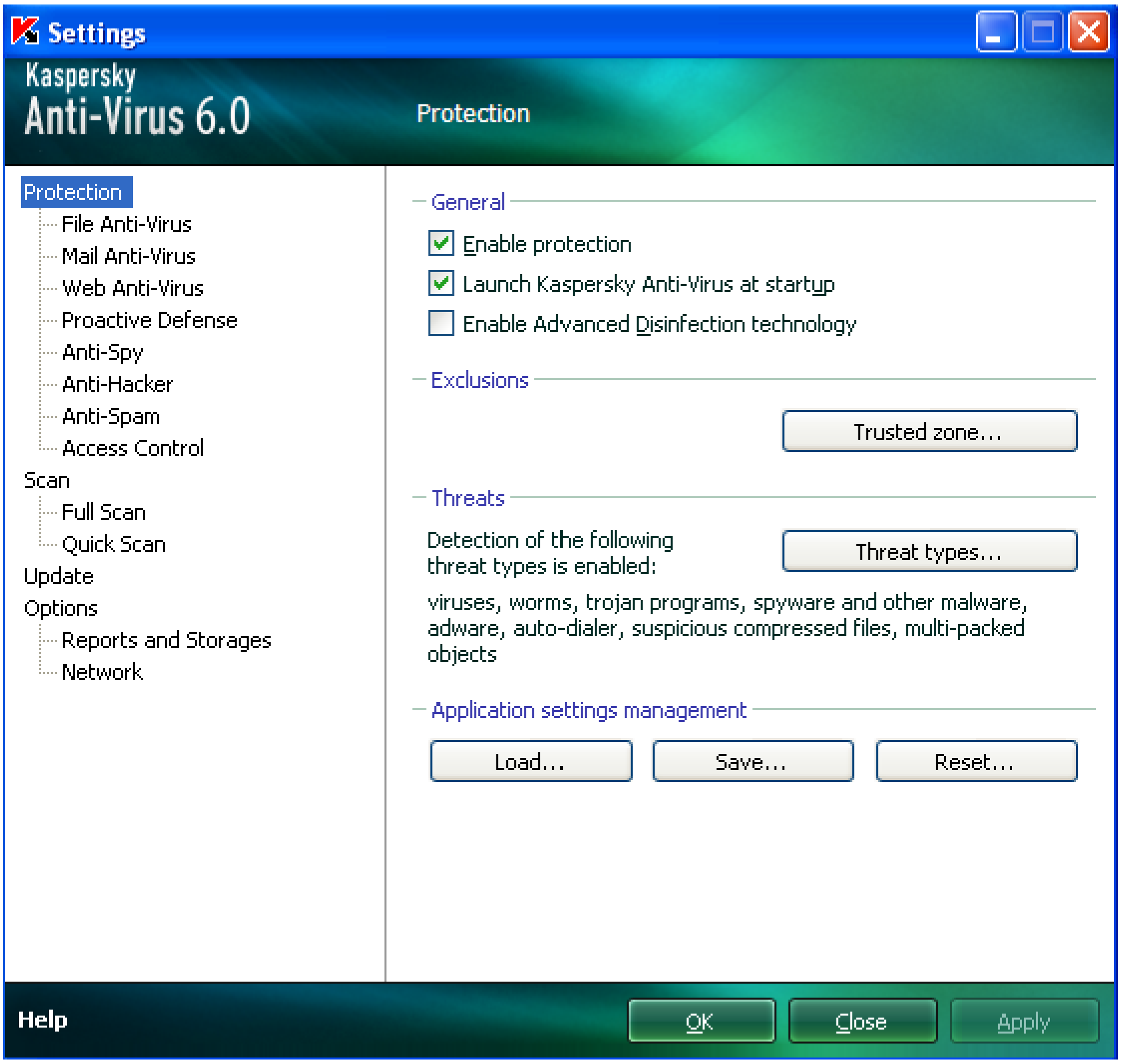
If you are updating from Kaspersky Lab web servers, try updating again. If the problem persists, contact Technical Support.

If you are updating from a different source, such as a local folder, we recommend updating it from Kaspersky Lab's web servers. If the error occurs again, contact Kaspersky Lab Technical Support.

File not in update source All files downloaded and installed on your computer during the update process are listed in a special file included in the update. This error occurs if there are any files on the update list that are not on the update source.
Error verifying signature This error might be returned by the application if the electronic digital signature of the update pack being downloaded is corrupted or does not match the Kaspersky Lab signature.
Index file corrupted or missing This error is generated if the .xml format index file used for updating is missing from the update source or corrupted.
ERRORS RELATED TO UPDATING USING KASPERSKY ADMINISTRATION KIT ADMINISTRATION SERVER These errors are generated in connection with problems updating the application through Kaspersky Administration Kit Administration Server. General recommendations: First, make sure that Kaspersky Administration Kit and its components (Administration Server and Network Agent) are installed and running. Try updating again. If this fails, restart Network Agent and Administration Server, then try updating again. If this does not resolve the issue, contact Technical Support.
Error connecting to Administration Server This error is generated if the Kaspersky Administration Kit Administration Server cannot be connected to. We recommend making sure that NAgent is installed and running.
Registration error in NAgent If this error occurs, follow the general recommendations for resolving this type of error. If the error reoccurs, send the detailed report file for the update and Network Agent on that computer to Technical Support Service using the online form. Describe the situation in detail.
Cannot establish connection. The Administration Server is busy and cannot process the request In this case, the update should be attempted later.
Cannot establish connection with Administration Server / Main Administration Server / NAgent, physical error / unknown error If you encounter such errors, we recommend trying to update again later. If the problem persists, contact Technical Support.
Error retrieving file from Administration Server, invalid transport argument If the error persists, contact Technical Support.
Error retrieving file from Administration Server If you encounter such errors, we recommend trying to update again later. If the problem persists, contact Technical Support.
VARIOUS CODES This group includes errors that cannot be included in any of the groups listed above.
Files for rollback operation missing This error is generated if another rollback attempt has been made after completing rollback of updates, but no updates had been made between them. The rollback procedure cannot be repeated until a successful update which restores a backup set of files has been performed.

CONFIGURING APPLICATION SETTINGS

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



☑ Enable protection

☑ Launch Kaspersky Anti-Virus at startup

□ Enable Advanced Disinfection technology

Detection of the following threat types is enabled:

viruses, worms, trojan programs, spyware and other malware, adware, auto-dialer, suspicious compressed files, multi-packed objects

Figure 9. Application settings configuration window

The window consists of two parts:

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

You can open this window:

- From the main application window. To do so, click the **Settings** button in the top part of the main window.
- From the context menu. To do so, select the **Settings** item from the application context menu.

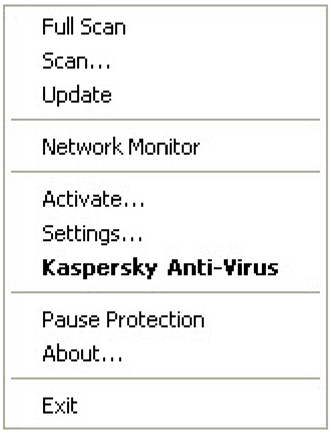


Figure 10. Context menu

- From the context menu for individual components. To do so, select the **Settings** item from the menu.

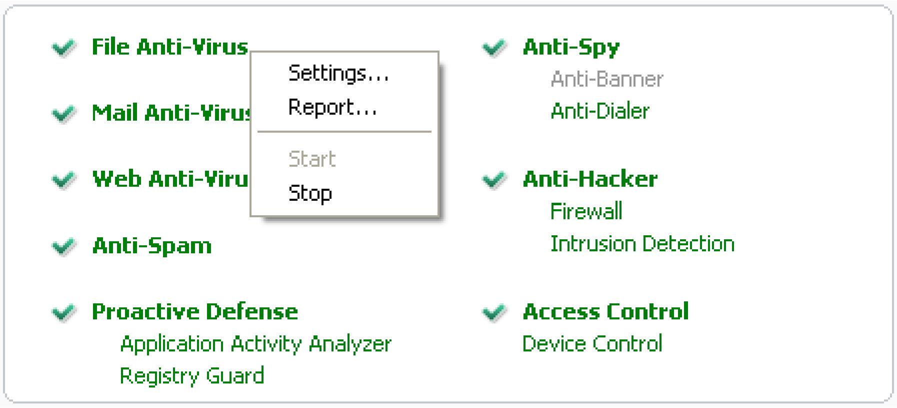


Figure 11. Opening the settings window from the context menu for an individual component

IN THIS SECTION

PROTECTION

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

- Enabling / disabling application protection (see page 144).
- Launching the application at the operation system startup (see page 145).
- Using advanced disinfection technology (see page 145).
- Selecting the detectable threat categories (see page 146).
- Creating a trusted zone (see page 146):
  - creating an exclusion rule (see page 147);
  - specifying additional exclusion settings (see page 148);
  - creating a list of trusted applications (see page 149);
  - exporting / importing trusted zone components (see page 150).
- Exporting / importing the application settings (see page 150).
- Restoring the default application settings (see page 151).

ENABLING / DISABLING COMPUTER PROTECTION

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

You can fully or partially disable the protection provided by the application.

The Kaspersky Lab specialists strongly recommend that you **do not disable protection**, since this could lead to an infection of your computer and data loss.

If you disable protection, all protection components will be disabled. This is indicated by:

- The inactive (grey) names of the disabled components in the main application window.
- The inactive (grey) application icon in the taskbar notification area.
- The red color of the security indicator.

In this case protection is being discussed in the context of the protection components. Disabling protection components does not affect the execution of virus scan tasks and updates of Kaspersky Anti-Virus.

➧ *To disable protection completely:*

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

LAUNCHING THE APPLICATION AT THE OPERATING SYSTEM STARTUP

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

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

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

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

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

USING ADVANCED DISINFECTION TECHNOLOGY

Today's malicious programs can invade the lowest levels of an operating system which makes them practically impossible to remove. Kaspersky Anti-Virus will ask you if you want to run the Advanced Disinfection Technology when it detects a threat currently active in the system. This will neutralize the threat and remove it from the computer.

After this procedure, you will need to restart your computer. After that, you are advised to run the full virus scan.

➧ *To start the advanced disinfection procedure, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. Check the ☑ **Enable Advanced Disinfection technology** box.

SELECTING DETECTABLE THREAT CATEGORIES

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

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

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

CREATING A TRUSTED ZONE

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

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

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

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

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

1. Open the application settings window.
2. In the left part of the window, select the **Protection** section.
3. In the **Exclusions** section, click the **Trusted zone** button.
4. In the window that will open, configure exclusion rules for objects (see page 147), and create the list of trusted applications (see page 149).

SEE ALSO

CREATING AN EXCLUSION RULE

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

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

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

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

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

Adding an exclusion creates a rule that can be used by several application components (File Anti-Virus, Mail Anti-Virus, Proactive Defense, Web Anti-Virus), and virus scan tasks .

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

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

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

1. Select the object from the report to add to the exclusions.

2. Select the **Add to Trusted zone** item from the context menu for this object.

3. The **Exclusion mask** window will open. Make sure that you are satisfied with the exclusion rule settings. Object name and relevant threat type fields are filled in automatically based on report data. To create the rule, click the **OK** button.

ADDITIONAL EXCLUSION SETTINGS

You can impose additional conditions of rule application for some objects by threat type. For example, it may be necessary to specify advanced settings in the following cases:

- *Invader (intrusion into the applications' processes)*. For this type of threat, you can give a name, mask, or complete path to the object being embedded (for example, a .dll file) as an additional exclusion condition.

- *Launching Internet Browser (launching the browser with certain settings)*. For this type of threat, you can specify browser startup settings as additional exclusion settings. For example, you can prevent browsers opening with certain settings while Proactive Defense is analyzing application activity. However, you want to allow the browser to open for the *www.kaspersky.com* domain with a link from Microsoft Office Outlook, as an exclusion rule. To do so, specify in the **Exclusion mask** window the Microsoft Office Outlook application as an exclusion **Object**, Launching Internet Browser as a **Threat type**, and enter an allowed domain mask in the **Comment** field.

ALLOWED FILE EXCLUSION MASKS

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

1. Masks without file paths:

   - ***.exe** – all files with the *.exe* extension;

   - ***.ex?** – all files with the *ex?* extension, where *?* may represent any single character;

   - **test** – all files with the name *test.*

2. Masks with absolute file paths:

   - **C:\dir\*.*** or **C:\dir\*** or **C:\dir\** – all files in the *C:\dir\* folder;

   - **C:\dir\*.exe** – all files with the .exe extension in the *C:\dir\* folder;

   - **C:\dir\*.ex?** – all files with the *ex?* extension in the *C:\dir\* folder where *?* may represent any character;

   - **C:\dir\test** – only the *C:\dir\test* file.

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

3. File path masks:

   - **dir\*.***, or **dir\***, or **dir\** – all files in all *dir\* folders;

   - **dir\test** – all *test* files in *dir\* folders;

   - **dir\*.exe** – all files with the *.exe* extension in all *dir\* folders;

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

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

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

SEE ALSO

Allowed exclusion masks according to the Virus Encyclopedia 149

ALLOWED EXCLUSION MASKS ACCORDING TO THE VIRUS ENCYCLOPEDIA

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

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

SEE ALSO

Allowed file exclusion masks 148

CREATING THE LIST OF TRUSTED APPLICATIONS

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

For example, you may feel that objects used by Microsoft Windows **Notepad** are safe and do not need to be scanned. In other words, you do trust this application. To exclude from scan the objects used by this process, add the **Notepad** application to the list of trusted applications. At the same time, the executable file and the trusted application's process will be scanned for viruses as they were before. To fully exclude the application from scan, you should use exclusion rules (see section "Creating an exclusion rule" on page 147).

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

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

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

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

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

EXPORTING / IMPORTING TRUSTED ZONE COMPONENTS

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

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

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

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

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

EXPORTING / IMPORTING KASPERSKY ANTI-VIRUS SETTINGS

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

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

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

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

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

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

RESTORING THE DEFAULT SETTINGS

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

In the window that will open, you will be asked to determine which settings and for which components should or should not be saved when restoring the recommended security level.

The list shows which components of Kaspersky Anti-Virus have settings which are different from the default value, either because they were changed by the user, or through accumulated training by the application (Firewall or Anti-Spam). If special settings have been created for any of the components, they will also be shown on the list.

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

These lists are populated gradually by using the program, based on individual tasks and security requirements, and creating them often takes much time. Therefore, we recommend saving them when you reset application settings.

After you are finished with the Configuration Wizard, the **Recommended** security level will be set for all components, except for the settings that you have decided to keep customized when restoring. In addition, the settings that you have specified when working with the Wizard will also be applied.

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

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

FILE ANTI-VIRUS

The **File Anti-Virus** component settings are grouped in the window (see section "Anti-virus protection of the computer file system" on page 43). By editing the application's settings, you can:

- change the security level (see page 45);
- change action to be performed on detected objects (see page 46);
- create a protection scope (see page 47);
- optimize the scan (see page 48);
- configure the scan of compound files (see page 48);

- change the scan mode (see page 50);
- use the heuristic analysis (see page 48);
- pause the component (see page 51);
- select a scan technology (see page 50);
- restore the default protection settings (see page 51) if they have been changed;
- disable File Anti-Virus.

➨ *To disable File Anti-Virus, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **File Anti-Virus** section.
3. Uncheck the ☑ **Enable File Anti-Virus** box in the right part of the window.

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

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

MAIL ANTI-VIRUS

The **Mail Anti-Virus** component settings are grouped in the window (see section "Mail Anti-Virus" on page 54). By editing the application's settings, you can:

- change the security level (see page 56);
- change action to be performed on detected objects (see page 56);
- create a protection scope (see page 57);
- change the scan methods (see page 58);
- use the heuristic analysis (see page 60);
- configure the scan of compound files (see page 60);
- configure filtering conditions for the objects attached to the email message (see page 61);
- restore default protection settings (see page 61);
- disable Mail Anti-Virus.

➨ *To disable Mail Anti-Virus, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Mail Anti-Virus** section.
3. Uncheck the ☑ **Enable Mail Anti-Virus** box in the right part of the window.

➧ *To proceed to the Mail Anti-Virus settings, please do the following:*

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

WEB ANTI-VIRUS

The **Web Anti-Virus** component settings are grouped in the window (see section "Web Anti-Virus" on page 63). By editing the application's settings, you can:

- change the security level (see page 65);
- change action to be performed on detected objects (see page 65);
- create a protection scope (see page 66);
- change the scan methods (see page 66);
- optimize the scan (see page 67);
- use the heuristic analysis (see page 67);
- restore the default Web Anti-Virus settings (see page 68);
- disable Web Anti-Virus.

➧ *To disable Web Anti-Virus, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Web Anti-Virus** section.
3. Uncheck the ☑ **Enable Web Anti-Virus** box in the right part of the window.

➧ *To proceed to the Web Anti-Virus settings, please do the following:*

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

PROACTIVE DEFENSE

The **Proactive Defense** component settings are grouped in this window (see section "Proactive Defense" on page 70). By editing the application's settings, you can:

- manage the list (see page 71) of dangerous activity;
- change the application's reaction to dangerous activity (see page 72) in the system;
- monitor system user accounts (see page 73);

- manage the list (see page 76) of system registry monitor rules;
- create rules for monitoring registry objects (see page 78);
- create groups of system registry objects to be monitored (see page 77);
- disable Application Activity Analyzer (see page 71) and Registry Guard modules (see page 76);
- disable Proactive Defense.

➡ *To disable Proactive Defense, please do the following:*

1. Open the application settings window.
2. In the left part of the window select the **Proactive Defense** section.
3. In the right part of the window, uncheck the ☑ **Enable Proactive Defense** box.

➡ *To disable **Application Activity Analyzer** or **Registry Guard**, please do the following:*

1. Open the application settings window.
2. In the left part of the window select the **Proactive Defense** section.
3. In the right part of the window uncheck the ☑ **Enable Application Activity Analyzer** or ☑ **Enable Registry Guard** boxes.

➡ *To proceed to editing the Proactive Defense settings, please do the following:*

1. Open the application settings window.
2. In the left part of the window select the **Proactive Defense** section.
3. In the right part of the window, in the **Application Activity Analyzer** section, or in the **Registry Guard** section, click the **Settings** button.

ANTI-SPY

The **Anti-Spy** component settings are grouped in this window (see section "Anti-Spy" on page 80). By editing the application's settings, you can:

- create the list of allowed banner addresses (see page 81);
- create the list of blocked banner addresses (see page 81);
- export / import lists of banner addresses (see page 82);
- create the list of trusted numbers (see page 82);
- disable the Anti-Banner (see page 80) and Anti-Dialer modules (see page 82);
- disable Anti-Spy.

➡ *To disable Anti-Spy, please do the following:*

1. Open the application settings window.
2. In the left part of the window select the **Anti-Spy** section.
3. In the right part of the window, uncheck the ☑ **Enable Anti-Spy** box.

➡ *To disable **Anti-Banner** or **Anti-Dialer**, please do the following:*

1. Open the application settings window.
2. In the left part of the window select the **Anti-Spy** section.
3. In the right part of the window, uncheck the ☑ **Enable Anti-Banner** (☑ **Enable Anti-Dialer**) box.

➡ *To proceed to editing the Anti-Spy settings, please do the following:*

1. Open the application settings window.
2. In the left part of the window select the **Anti-Spy** section.
3. In the right part of the window, in the **Anti-Banner** section, or in the **Anti-Dialer** section, click the **Settings** button.

ANTI-HACKER

The **Anti-Hacker** component settings are grouped in this window (see section "Protection against network attacks" on page 84). By editing the application's settings, you can:

- change Anti-Hacker protection level (see page 86);
- create the rules for applications manually (see page 87) and using a template (see page 88);
- create rules for packet filtering (see page 88);
- change the rule priority (see page 89);
- export / import the rules (see page 90);
- fine-tune the rules for applications and packets (see page 90);
- create rules for security zones (see page 93);
- change the security zone status (see page 94);
- enable / disable the stealth mode (see page 95);
- change Firewall mode (see page 95);
- disable the Firewall and Intrusion Detection System modules (see page 96);
- disable Anti-Hacker.

➡ *To disable Anti-Hacker, please do the following:*

1. Open the application settings window.
2. Select the **Anti-Hacker** section in the left part of the window.
3. Uncheck the ☑ **Enable Anti-Hacker** box in the right part of the window.

➡ *To disable **Firewall** or **Intrusion Detection System**, please do the following:*

1. Open the application settings window.
2. Select the **Anti-Hacker** section in the left part of the window.

3. Uncheck the ☑ **Enable Firewall** box or the ☑ **Enable Intrusion Detection System** box in the right part of the window.

➧ *To proceed to editing the Anti-Hacker settings, please do the following:*

1. Open the application settings window.

2. Select the **Anti-Hacker** section in the left part of the window.

3. In the right part of the window, click the **Settings** button in the **Firewall** section.

ANTI-SPAM

The **Anti-Spam** component settings are grouped in this window (see section "Anti-Spam" on page 100). By editing the application's settings, you can:

- change the sensitivity level (see page 105);
- use the Mail Dispatcher (see page 106);
- exclude Microsoft Exchange Server messages from the scan (see page 107);
- change the scan methods (see page 107);
- select the spam filtering technology (see page 108);
- define spam and potential spam factors (see page 108);
- use additional spam filtering features (see page 109);
- create the list of allowed senders (see page 110);
- create the list of allowed phrases (see page 110);
- import the list of allowed senders (see page 111);
- create the list of blocked senders (see page 111);
- create the list of banned phrases (see page 112);
- configure spam processing in Microsoft Office Outlook (see page 113), Microsoft Outlook Express (Windows Mail) (see page 115), The Bat! (see page 115);
- train Anti-Spam using the Training Wizard (see page 103), on outgoing e-mail messages (see page 104), using e-mail client (see page 104), with reports (see page 105);
- disable Anti-Spam.

➧ *To disable Anti-Spam, please do the following:*

1. Open the application settings window.

2. In the left part of the window, select the **Anti-Spam** section.

3. Uncheck the ☑ **Enable Anti-Spam** box in the right part of the window.

➧ *To proceed to editing the Anti-Spam settings, please do the following:*

1. Open the application settings window.

2. In the left part of the window, select the **Anti-Spam** section.

3. In the right part of the window, in the **Sensitivity** section, click the **Customize** button.

SCAN

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

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

Scan

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

Full Scan

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

Quick Scan

Virus scan of operating system startup objects.

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

- select the security level (see page 123) with the settings that the task will use;
- select an action (see page 123) that the application will apply when it detects an infected / potentially infected object;
- create a schedule (see page 128) to run tasks automatically;
- specify the file types (see page 124) to be scanned for viruses;
- specify the scan settings for compound files (see page 126);
- select scan methods and scan technologies (see page 126);
- assign common scan settings to all tasks (see page 129).

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

1. Open the application settings window.

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

3. In the right part of the window, select the required security level, the reaction to the threat and configure the run mode. Click the **Customize** button in order to switch to the settings of other tasks' settings. To restore the default settings, click the **Default level** button.

UPDATE

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

- the source (see page 133) from which updates will be downloaded and installed;
- the application update run mode (see page 136) and the specific components to be updated (see page 136);

- how often the update will be launched if scheduled launch is configured (see page 135);
- which account (see page 135) the update will be launched under;
- if the updates are to be copied to a local source (see page 137);
- use of a proxy server (see page 134).

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

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

OPTIONS

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

- Application self-defense (see page 158).
- Restricting the access to the application (see page 159).
- Using the application on a laptop (see page 159).
- Limiting the size of iSwift files (see page 160).
- Notifications about Kaspersky Anti-Virus events (see page 160):
  - selecting event type and way of sending notifications (see page 161);
  - configuring email notification (see page 161);
  - configuring the event log (see page 162).
- Active interface elements (see page 162).

APPLICATION SELF-DEFENSE

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

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

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

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

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

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

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

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

RESTRICTING ACCESS TO THE APPLICATION

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

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

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

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

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

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

USING THE APPLICATION ON A LAPTOP

To save power (battery charge) on a portable computer, scan and update tasks may be postponed.

Since both scanning a computer for viruses and updating the application may require significant resources and time, we recommend that you disable scheduled start of these tasks. This will allow you to save the battery charge. If necessary, you can update the application or start a virus scan manually.

➡ *To use the battery saving service, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Options** section.
3. In the **Resources** section, check the ☑ **Disable scheduled tasks while running on battery power** box.

RESTRICTING THE SIZE OF ISWIFT FILES

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

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

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

NOTIFICATIONS ABOUT KASPERSKY ANTI-VIRUS EVENTS

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

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

Notifications can be delivered in one of the following ways:

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

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

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

SEE ALSO

SELECTING EVENT TYPE AND WAY OF SENDING NOTIFICATIONS

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

- **Critical notifications** are events of critical importance. It is highly recommended that they are reported of with notifications since they point to problems in the application's operation or gaps in your computer's protection. For example, *databases are obsolete* or *license validity period has expired*.

- **Error notifications** are events that lead to the application's inoperability. For example, *databases are missing or corrupted*.

- **Important notifications** are events that should be attended to because they reflect important situations in the application's operation. For example, *databases are obsolete* or *license expires soon*.

- **Minor notifications** are reference-type messages that do not contain important information, as a rule. For example, *object quarantined*.

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

1. Open the application settings window.

2. In the left part of the window, select the **Options** section.

3. In the **Appearance** section, check the ☑ **Enable notifications** box and click the **Settings** button.

4. In the **Notification settings** window that will open, check the ☑ boxes for the events and the ways of sending notifications for them, which you want to be notified of.

CONFIGURING NOTIFICATION BY EMAIL

After you have selected the events (see section "Selecting event type and way of sending notifications" on page 161) about which you wish to receive a notification by email, you should set up notifications.

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

1. Open the application settings window.

2. In the left part of the window, select the **Options** section.

3. In the **Appearance** section, check the ☑ **Enable notifications** box and click the **Settings** button.

4. In the **Notification Settings** window that will open, check the ☑ boxes for the required events in the **Email** field and click the **Email settings** button.

5. In the **Email notification settings** window that will open, specify the required values for the settings. If you want notifications about events to be sent at scheduled times, create a schedule for sending the information message by clicking the **Change** button. Make the required changes in the **Schedule** window that will open.

CONFIGURING EVENT LOG

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

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

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

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

ACTIVE INTERFACE ELEMENTS

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

Animate taskbar notification area icon.

Depending on the operation being performed by the application, the application icon in the system tray will change. For example, when scanning email messages, a small letter icon appears in front of the application icon. By default, the application icon is animated. In this case, the icon only displays the protection status of your computer: if the protection is enabled, the icon is in full color; if the protection is paused or disabled, the icon turns grey.

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

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

If the application is installed on a computer running under Microsoft Windows Vista, this option will be unavailable.

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

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

REPORTS AND STORAGES

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

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

In this section, you can:

- configure the report creation and storage (see page 164);
- configure quarantine and backup (see page 166);
- clear the report archive, Quarantine and Backup.

To clear the storage areas, please do the following:

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

SEE ALSO

PRINCIPLES OF HANDLING REPORTS

The operation of each Kaspersky Anti-Virus's component and the execution of each virus scan or update task are recorded in a report.

To view reports, please do the following:

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

To review all the events in a component's operation or in a task execution recorded in the report, please do the following:

1. Open the main application window and click the **Reports** button.
2. In the window that will open, on the **Reports** tab, select the name of a component or a task and click the **Details** link. As a result a window will pop up, containing detailed information on the performance of the selected component or task. The resulting statistics on performance are displayed in the upper part of the window, and detailed information is given on the various tabs in the central part. Depending on the component or task, the composition of the tabs can vary.

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

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

2. In the window that will open, on the **Reports** tab, select the name of a component or a task and click the **Details** link.

3. In the window that will open the information about the performance of selected component or task will be shown. Click the **Save As** button and specify where you want to save the report file.

CONFIGURING REPORTS

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

- Allow or block logging informative events. As a rule, those events are not critical for the protection (the ☑ **Log non-critical events** box).

- Allow the saving in the report only for the events that have occurred since the last startup of the task. This saves disk space by reducing the report size (the ☑ **Keep only recent events** box). If the box is checked, the information will be updated every time the task is restarted. However, only non-critical information will be overwritten.

- Set the storage term for reports (the ☑ **Store reports no longer than** box). By default, the objects storage time is 14 days; once it expires, the objects will be deleted. You can change the maximum storage time, or even cancel any restrictions imposed on it.

- Specify the maximum report size (the ☑ **Maximum size** box). By default, the maximum size is 100 MB. You can cancel any restrictions imposed on the report's size, or enter another value.

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

1. Open the application settings window.

2. In the left part of the window, select the **Reports and Storages** section.

3. In the **Reports** section, check all required boxes, and set the storage term and the maximum size of the report, if necessary.

QUARANTINE FOR POTENTIALLY INFECTED OBJECTS

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

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

Why are some objects considered as *potentially inflected*? It is not always possible to exactly determine whether an object is infected. This could be for the following reasons:

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

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

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

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

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

A potentially infected object can be detected and quarantined when being scanned for viruses, or by File Anti-Virus, Mail Anti-Virus, or Proactive Defense.

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

SEE ALSO

Actions on quarantined objects 165

Configuring quarantine and backup 166

ACTIONS ON QUARANTINED OBJECTS

You can do the following operations with quarantined objects:

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

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

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

BACKUP COPIES OF DANGEROUS OBJECTS

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

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

Backup is a special repository that contains backup copies of dangerous objects after processing or deletion. The main function of backup is the ability to restore the original object at any time. Files in backup are saved in a special format and are not dangerous.

SEE ALSO

Working with backup copies 165

Configuring quarantine and backup 166

WORKING WITH BACKUP COPIES

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

- restore selected copies;

- delete objects.

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

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

2. In the window that will open, on the **Backup** tab, take the required actions.

CONFIGURING QUARANTINE AND BACKUP

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

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

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

- Determine the maximum storage time for quarantined objects and for copies of objects in the backup (the ☑ **Store objects no longer than** box). By default, the objects storage time is 30 days; once it expires, the objects will be deleted. You can change the maximum storage time, or even cancel any restrictions imposed on it.

- Specify the maximum size of data storage area (the ☑ **Maximum size** box). By default, the maximum size is 250 MB. You can cancel any restrictions imposed on the report's size, or enter another value.

➧ To configure the quarantine and backup settings:

1. Open the application settings window.

2. In the left part of the window, select the **Reports and Storages** section.

3. In the **Quarantine and Backup** section, check the required boxes and specify the maximum size of data storage area, if necessary.

NETWORK

The section contains settings allowing to:

- create a list of ports to be monitored (see page 166);

- enable / disable the encrypted connection scan mode (via SSL protocol) (see page 167).

CREATING A LIST OF PORTS TO BE MONITORED

Such protection components as Mail Anti-Virus, Web Anti-Virus, Anti-Hacker, Anti-Spam, monitor the data streams transferred via specific protocols and passing via certain open ports on your computer. Thus, for example, Mail Anti-Virus analyzes information transferred via the SMTP protocol, and Web Anti-Virus analyzes HTTP packets.

You can select one of two port monitoring modes:

- **Monitor all ports**.

- **Monitor selected ports only**. A list of ports that are used for transmitting email and HTTP traffic is included with the application installation package.

You can add a new port or disable monitoring for a certain port, thereby disabling analysis of the traffic passing through that port for dangerous objects.

For example, there is a nonstandard port on your computer through which data is exchanged with a remote computer using HTTP protocol. Web Anti-Virus monitors HTTP traffic. To analyze this traffic for malicious code, you can add this port to the list of monitored ports.

> When any of its components starts, Kaspersky Anti-Virus opens port 1110 as a listening port for all incoming connections. If that port is reserved at the time, it selects 1111, 1112, etc., as a listening port.

If you use Kaspersky Anti-Virus and another vendor's firewall simultaneously, you should configure that firewall to allow the *avp.exe* process (internal Kaspersky Anti-Virus process) on all the ports listed above.

For example, your firewall contains a rule for *iexplorer.exe* that allows for establishing connections on port 80. However, when Kaspersky Anti-Virus intercepts the connection query initiated by *iexplorer.exe* on port 80, it transfers it to *avp.exe*, which in turn attempts to establish connection with the web page independently. If there is no allow rule for *avp.exe*, the firewall will block the query. The user will then be unable to access the webpage.

➡ *In order to add a port to the list of monitored ports:*

1. Open the application settings window.
2. In the left part of the window, select the **Network** section.
3. In the **Monitored ports** section click the **Port settings** button.
4. In the **Port settings** window that will open, click the **Add** button.
5. In the **Port** window that will open, specify the required data.

➡ *In order to exclude a port from the list of monitored ports:*

1. Open the application settings window.
2. In the left part of the window, select the **Network** section.
3. In the **Monitored ports** section click the **Port settings** button.
4. In the **Port settings** window that will open, uncheck the box next to the port's description.

SCANNING ENCRYPTED CONNECTIONS

Connecting using the Secure Sockets Layer (SSL) protocol protects data exchange channel on the Internet. The SSL protocol allows identifying the parties that exchange data using electronic certificates, encoding the data being transferred, and ensuring their integrity in the course of the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus programs do not scan SSL traffic.

Kaspersky Anti-Virus verifies secure connections using Kaspersky Lab certificate. This certificate will always be used to check whether the connection is secure.

Further traffic scans via the SSL protocol will be performed using the installed Kaspersky Lab's certificate. If an invalid certificate is detected when you connect to the server (for example, if the certificate is replaced by an intruder), a notification will be displayed with suggestions to either accept or reject the certificate, or view the certificate information.

➡ *To enable encrypted connections scan, please do the following:*

1. Open the application settings window.
2. In the left part of the window, select the **Network** section.

3. In the **Encrypted connections** section, check the ☑ **Scan encrypted connections** box and click the **Install certificate** button.

4. In the window that will open, click the **Install Certificate** button. This will start a wizard with instructions to follow for a successful installation of the certificate.

The automatic installation of the certificate will only work with Microsoft Internet Explorer. To scan encrypted connections in Mozilla Firefox (see page 168) and Opera (see page 169), you should install a Kaspersky Lab certificate manually.

SEE ALSO

SCANNING ENCRYPTED CONNECTIONS IN MOZILLA FIREFOX

Mozilla Firefox browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Firefox, you should install the Kaspersky Lab's certificate manually.

To install the Kaspersky Lab's certificate, please do the following:

1. In the browser's menu, select the **Tools** → **Options** item.

2. In the window that will open, select the **Advanced** section.

3. In the **Certificates** section, select the **Security** tab and click the **Manage Certificates** button.

4. In the window that will open, select the **Certification Centers** tab and click the **Restore** button.

5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. In the window that will open, check the boxes to select the actions which will be validated with the installed certificate. To view information about the certificate, click the **View** button.

To install the Kaspersky Lab's certificate for Mozilla Firefox version 3.x, please do the following:

1. In the browser's menu, select the **Tools** → **Options** item.

2. In the window that will open, select the **Additional** section.

3. On the **Encryption** tab, click the **Viewing certificates** button.

4. In the window that will open, select the **Certification Centers** tab and click the **Import** button.

5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. In the window that will open, check the boxes to select the actions which will be validated with the installed certificate. To view information about the certificate, click the **View** button.

If your computer is running under Microsoft Windows Vista operating system, the path to Kaspersky Lab certificate file will be: *%AllUsersProfile%\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SCANNING ENCRYPTED CONNECTIONS IN OPERA

Opera browser does not use Microsoft Windows certificate storage. To scan SSL connections when using Opera, you should install the Kaspersky Lab's certificate manually.

➧ *To install the Kaspersky Lab's certificate, please do the following:*

1. In the browser's menu, select the **Tools** → **Preferences** item.
2. In the window that will open, select the **Advanced** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that will open, select the **Vendors** tab and click the **Import** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that will open, click the **Install** button. Kaspersky Lab's certificate will be installed. To view information about the certificate, and to select actions for which the certificate will be used, select the certificate in the list and click the **View** button.

➧ *To install the Kaspersky Lab's certificate for Opera version 9.x, please do the following:*

1. In the browser's menu, select the **Tools** → **Preferences** item.
2. In the window that will open, select the **Advanced** section.
3. In the left part of the window, select the **Security** tab and click the **Manage Certificates** button.
4. In the window that will open, select the **Certification Centers** tab and click the **Import** button.
5. In the window that will open, select the Kaspersky Lab's certificate file. The path to the Kaspersky Lab's certificate file is as follows: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP60MP4\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. In the window that will open, click the **Install** button. Kaspersky Lab's certificate will be installed.

RESCUE DISK

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

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

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

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

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

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

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

➡ *To create a Rescue Disk, please do the following:*

1. Open the main application window.
2. Click the **Rescue Disk** button to run the Rescue Disk Creation Wizard (see page 170).
3. Follow the Wizard instructions.
4. Using the file provided by the wizard, create a boot CD/DVD. To do so, you can use any CD/DVD burning application, such as Nero.

SEE ALSO

Creating the Rescue Disk 170

Booting the computer using the Rescue Disk 172

CREATING THE RESCUE DISK

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

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

The image file created by the wizard will be saved in the "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP80\Data\Rdisk\"* folder (or "*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk\"* – for Microsoft Vista) named as *rescuecd.iso*. If the wizard has detected an ISO file created earlier in the specified folder, you can use it as original disk image by checking the ☑ **Use existing ISO file** box, and jump to Step 3 – image update (see page 240). If the wizard has not detected any image file, this box is not available.

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

DETAILED DISCUSSION OF THE WIZARD STEPS

STEP 1. SELECT RESCUE DISK IMAGE SOURCE

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

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

- Select ● **Copy ISO image from CD/DVD disk or local network** if you already have a Rescue Disk on CD/DVD or an image prepared for it and stored on your computer or on a local network resource.

- Select the ● **Download ISO image from Kaspersky Lab server** option if you do not have any existing image file, you can download it from a Kaspersky Lab's server (file size is about 100 MB).

STEP 2. COPYING ISO IMAGE

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

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

STEP 3. ISO IMAGE UPDATE

File update procedure includes:

- update of application databases;

- update of configuration files.

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

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

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

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

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

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

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

STEP 4. REMOTE STARTUP

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

Enter the information about the computer:

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

The next wizard window is an iAMT console where you can control the computer loading process (see page 172).

STEP 5. CLOSING THE WIZARD

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

BOOTING THE COMPUTER USING THE RESCUE DISK

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

You will need the boot disk image file (.iso) to load the operating system. You can download (see page 171) the file from a Kaspersky Lab's server or update (see page 240) the existing one.

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

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

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

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

   File system mounting may result in its corruption.

3. Searching the Microsoft Windows swap file *pagefile.sys*. If it is missing, the volume of the virtual memory is limited by the size of the RAM.

4. Selecting the localization language. If the selection has not been done after a lapse of time, then the English language will be set by default.

   When loading a remote computer, this step is skipped.

5. Searching (creating) the folders for anti-virus databases, reports, quarantine storage, and additional files. By default the folders of Kaspersky Lab's application installed on the infected computer (*ProgramData/Kaspersky Lab/AVP8* - for Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* - for earlier versions of Microsoft Windows) will be used. If such application folders cannot be found, an attempt to create them will be made. If those folders have not been found, and they cannot be created, the *kl.files* folder will be created on a system disk.

6. Trying to configure network connections based on data found in system files of the computer being loaded.

7. Loading graphical subsystem and starting Kaspersky Rescue Disk (when loading the computer from a CD/DVD).

   If a remote computer is loaded in the iAMT console, the command prompt will be loaded. You can use the commands for working with Kaspersky Rescue Disk from the command line to manage tasks (see page 174).

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

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

1. In BIOS settings enable booting from CD/DVD-ROM (for detailed information please refer to the documentation for the motherboard installed on your computer).

2. Insert the CD/DVD with Rescue Disk image into the CD/DVD drive of an infected computer.

3. Restart your computer.

4. Further the boot continues according with the algorithm described above.

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

1. Open the main application window.

2. Click the **Rescue Disk** button to run the Rescue Disk Creation Wizard (see page 170). Follow the Wizard instructions.

   Note that you should select the ● **Remote startup** option at the disk image update stage (see page 240).

Further the boot continues according with the algorithm described above.

WORKING WITH KASPERSKY RESCUE DISK FROM THE COMMAND PROMPT

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

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

Command line syntax:

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

The following may be used as commands:

HELP	help with command syntax and list of commands
SCAN	scan objects for viruses
UPDATE	update task start
ROLLBACK	last update rollback
EXIT	exit Kaspersky Rescue Disk

IN THIS SECTION

VIRUS SCAN

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

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

Settings description:

<object to scan> – this parameter gives the list of objects that will be scanned for malicious code. The parameter may include several space-separated values from the list provided.

<files>	List of paths to the files and/or folders to be scanned. You can enter an absolute or relative path to the file. Items on the list are separated by a space. Comments: • if the name of the object contains a space, it should be supplied with quotation marks; • if reference is made to a specific directory, all files in the directory are scanned.
/discs/	Scanning all drives.
/discs/<disc_name>:/<folder>	Scanning the selected drive, where <disc_name> is the name of the drive, and <folder> is the path to the folder being scanned.
<action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for -**i8.**	
-i0	Take no action on the object; simply record information about it in the report.
-i1	Treat infected objects and if disinfection is impossible, skip.
-i2	Treat infected objects, and if disinfection fails, delete. Do not delete infected objects from compound objects. Delete infected compound objects with executable headers (.sfx archives) (this is the default setting).
-i3	Treat infected objects and if disinfection fails, delete. Delete all compound objects completely if infected parts cannot be deleted.
-i4	Delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.
-i8	Prompt the user for action if an infected object is detected.
-i9	Prompt the user for action at the end of the scan.
<file types> – this parameter defines the file types that will be subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents will be scanned.	
-fe	Scan only infected files by extension.
-fi	Scan only infected files by contents.
-fa	Scan all files.
<exclusions> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.	

-e:a	Do not scan archives.
-e:b	Do not scan email databases.
-e:m	Do not scan plain text emails.
-e:<filemask>	Do not scan objects, which match the mask.
-e:<seconds>	Skip objects that are scanned for longer than the time specified in the **<seconds>** parameter.
-es:<size>	Skip objects of size (in MB) exceeding the value specified in the **<size>** parameter.

Examples:

➧ *Start scan of the Documents and Settings folder and the <D> drive:*

```
SCAN /discs/D: "/discs/C:/Documents and Settings"
```

KASPERSKY ANTI-VIRUS UPDATE

The command for updating Kaspersky Anti-Virus's databases and program modules features the following syntax:

```
UPDATE [<update_source>] [-R[A]:<report_file>]
```

Settings description:

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

Examples:

➧ *Update databases and record all events in a report:*

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
ROLLBACK [-R[A]:<report_file>]
```

Settings description:

-R[A]:<report_file>	**-R:<report_file> –** log only important events in the report. **-RA:<report_file> –** log all events in the report. An absolute path to the file is allowed to use. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

Example:

```
ROLLBACK -RA:/discs/C:/rollback.txt
```

VIEWING HELP

Use this command to view the application command line syntax:

```
[ -? | HELP ]
```

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

```
<command> -?

HELP <command>
```

VALIDATING KASPERSKY ANTI-VIRUS SETTINGS

After Kaspersky Anti-Virus has been installed and configured, you can verify whether the application is configured correctly, using a test "virus" and its modifications. A separate test is required for each protection component / protocol.

IN THIS SECTION

TEST "VIRUS" EICAR AND ITS MODIFICATIONS

This test "virus" was specially developed by eicar (The European Institute for Computer Antivirus Research) for the testing of anti-virus products.

The test "virus" IS NOT A VIRUS, because it does not contain code that can harm your computer. However, most anti-virus products identify this file as a virus.

Never use real viruses for testing the operation of an anti-virus product!

You can download this test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

Before you download the file, you must disable the computer's anti-virus protection, because otherwise the application would identify and process the file *anti_virus_test_file.htm* as an infected object transferred via the HTTP protocol. Do not forget to enable the anti-virus protection immediately after you download the test "virus".

The application identifies the file downloaded from the **EICAR** site as an infected object containing a virus that **cannot be disinfected** and performs the actions specified for this type of object.

You can also modify the standard test "virus" to verify the operation of the application. To modify the "virus", change the content of the standard "virus" by adding one of the prefixes to it (see table below). To modify test "virus", you can use any text or hypertext editor, such as **Microsoft Notepad**, **UltraEdit32**, etc.

You can test the correctness of the operation of the anti-virus application using the modified EICAR "virus" only if your anti-virus bases were last updated on or after October 24, 2003 (October, 2003 cumulative updates).

In the table below, the first column contains the prefixes that must be added at the start of the standard test "virus" string. The second column lists all possible statuses that the Anti-Virus application can assign to the object, based on the results of the scan. The third column indicates how the application processes objects with the specified status. Please note that that actual actions performed on the objects are determined by the application's settings.

After you have added a prefix to the test "virus", save the new file under a different name, for example: *eicar_dele.com*. Assign similar names to all modified "viruses".

Table 1. Modifications of the test "virus"

Prefix	Object status	Object processing information
No prefix, standard test "virus".	**Infected**. Object contains code of a known virus. You cannot disinfect the object.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed will be that specified for non-disinfectable objects.
CORR–	**Corrupted**.	The application could access the object but could not scan it because it is corrupted (for example, the file structure is corrupted, or the file format is invalid). You can find the information that the object has been processed in the report on application operation.
WARN–	**Suspicious**. Object contains code of an unknown virus. You cannot disinfect the object.	The object has been found suspicious by the heuristic code analyzer. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
SUSP–	**Suspicious**. Object contains modified code of a known virus. You cannot disinfect the object.	The application detected a partial correspondence of a section of object code with a section of code of a known virus. At the time of detection, the Anti-Virus threat signature databases contain no description of the procedure for treating this object. You will be notified when an object of this type is detected.
ERRO–	**Scanning error**.	An error occurred during a scan of an object. The application could not access the object, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is scanned on a network resource). You can find the information that the object has been processed in the report on application operation.
CURE–	**Infected**. Object contains code of a known virus. Disinfectable.	Object contains a virus that can be disinfected. The application will disinfect the object; the text of the "virus" body will be replaced with the word CURE. You will be notified when an object of this type is detected.
DELE–	**Infected**. Object contains code of a known virus. You cannot disinfect the object.	The application identifies the object as a non-disinfectable virus. An error occurs while attempting to disinfect the object; the action performed will be that specified for non-disinfectable objects. You will be notified when an object of this type is detected.

TESTING THE HTTP TRAFFIC PROTECTION

➨ *In order to verify that viruses are successfully detected in data stream transferred via the HTTP protocol, please do the following:*

Try to download this test "virus" from the **EICAR**'s official website at http://www.eicar.org/anti_virus_test_file.htm.

When the computer attempts to download the test "virus", Kaspersky Anti-Virus will detect the object, identify it as an infected object that cannot be disinfected, and will perform the action specified in the HTTP traffic settings for objects with this status. By default, when you attempt to download the test "virus", the connection with the website will be terminated and the browser will display a message indicating that the object is infected with the EICAR-Test-File virus.

TESTING THE SMTP TRAFFIC PROTECTION

In order to detect viruses in data streams transferred using SMTP protocol, you must use an email system that uses this protocol to transfer data.

We recommend that you test how the Anti-Virus handles outgoing email messages, including both the body of the message and attachments. To test detection of viruses in the body of the message, copy the text of the standard test "virus" or of the modified "virus" into the body of the message.

➡ *To do so:*

1. Create a message in the **Plain text** format using the mail client installed on your computer.

   A message that contains a test virus will not be scanned if it is created in RTF or HTML format!

2. Copy the text of the standard or modified "virus" at the beginning of the message, or attach a file containing the test "virus" to the message.
3. Send the message to the administrator.

The application will detect the object, identify it as infected, and block the message.

VALIDATING FILE ANTI-VIRUS SETTINGS

➡ *To verify the correctness of File Anti-Virus configuration, please do the following:*

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR**'s website (http://www.eicar.org/anti_virus_test_file.htm), as well as all the test "virus" modifications you have created.
2. Allow all events to be logged so the report file retains data on corrupted objects or objects skipped due to errors.
3. Run the test "virus" or one of its modified versions.

The File Anti-Virus will intercept the call to execute the file, scan it, and perform the action specified in the settings for objects of that status. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view information about the results of the File Anti-Virus operation in the report about the component's operation.

VALIDATING VIRUS SCAN TASK SETTINGS

➡ *In order to verify that the virus scan task is correctly configured:*

1. Create a folder on the disk. Copy into this folder the test "virus" downloaded from the official **EICAR**'s website (http://www.eicar.org/anti_virus_test_file.htm), as well as all the test "virus" modifications you have created.
2. Create a new virus scan task and select the folder, containing the set of test "viruses", as the object to scan.
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors.
4. Run the virus scan task.

When the scan task is running, the actions specified in the task settings will be performed as suspicious or infected objects are detected. By selecting different actions to be performed with the detected object, you can perform a full check of the component's operation.

You can view all information about the virus scan task actions in the report on the component's operation.

VALIDATING ANTI-SPAM SETTINGS

You can use a test message identified as SPAM to test the anti-spam protection.

The body of the test message must contain the following line:

```
Spam is bad do not send it
```

After this message is received on the computer, Kaspersky Anti-Virus will scan it, assign it the "spam" status, and perform the action specified for objects of this type.

TYPES OF NOTIFICATIONS

When Kaspersky Anti-Virus events occur, special notification messages are displayed. Depending on how critical the event is for computer security, you might receive the following types of notifications:

- **Alarm**. A critical event has occurred, for instance, a malicious object or dangerous activity has been detected on your system. You should immediately decide how to deal with this threat. This type of notification is color-coded in red.
- **Warning**. A potentially dangerous event has occurred. For instance, potentially infected files or suspicious activity have been detected on your system. You should decide how dangerous you think this event is. This type of notification is color-coded in yellow.
- **Info**. This notification gives information about non-critical events. This notification type includes, for example, notifications that pop up during Anti-Hacker training. Informational notifications are color coded in blue.

IN THIS SECTION

MALICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects malicious code, a special notification will pop up.

It contains:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Disinfect** – attempt to disinfect the malicious object. Before treatment, a backup copy is made of the object in case the necessity arises to restore it or a portrait of its infection.
- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but take no actions on it; simply record information about it in a report.

  You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

OBJECT CANNOT BE DISINFECTED

There are some cases when it is impossible to disinfect a malicious object. This could happen if a file is so damaged that it is impossible to delete malicious code from it and restore integrity. The treatment procedure cannot be applied to several types of dangerous objects, such as Trojans.

In such cases, a special notification will pop up containing:

- Threat type (for instance, *virus*, *Trojan*) and the name of the malicious object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the malicious object and a path to it.

You are asked to select one of the following responses to the object:

- **Delete** – delete malicious object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but take no actions on it; simply record information about it in a report.

  You can later come back to skipped malicious objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted or the time from beginning a virus scan task until it is complete.

SPECIAL TREATMENT REQUIRED

When you detect a threat that is currently active in the system (for example, a malicious process in RAM or in startup objects), a message will pop up prompting you to carry out a special advanced disinfection procedure.

The Kaspersky Lab specialists strongly recommend that you agree with to carry out the advanced disinfection procedure. To do so, click the **OK** button. However, note that your computer will restart once the procedure is complete, so we recommend saving your current work and closing all applications before running the procedure.

While the disinfection procedure is running, email client or operating system registry editing sessions cannot be started. After restarting your computer, you are advised to run the full virus scan.

SUSPICIOUS OBJECT DETECTED

If File Anti-Virus, Mail Anti-Virus, or a virus scan detects an object containing code from an unknown virus or modified code of a known virus, a special notification will pop up.

It contains:

- The threat type (for instance, *virus*, *Trojan*) and the name of the object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the dangerous object is given as a link to www.viruslist.com, where you can find more detailed information on the type of threat detected on your computer.
- Full name of the object and a path to it.

You are asked to select one of the following responses to the object:

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

  When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

  > If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

- **Delete** – delete the object. Before deleting, a backup copy of the object is created in case the necessity arises to restore it or a portrait of its infection.
- **Skip** – block access to the object but take no actions on it; simply record information about it in a report.

  You can later come back to skipped objects in the report window. However, you cannot postpone processing objects detected in emails.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

If you are sure that the object detected it is not malicious, we recommend adding it to the trusted zone to avoid the program making repeat false positives when you use the object.

DANGEROUS OBJECT DETECTED IN TRAFFIC

When Web Anti-Virus detects a malicious object in traffic, a special notification pops up on screen.

The notification contains:

- The threat type (for instance, *virus modification*) and the name of the dangerous object as listed in the Kaspersky Lab Virus Encyclopedia. The name of the object is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.

- Full name of the dangerous object and a path to the webpage.

You are asked to select one of the following responses to the object:

- **Allow** – continue the object downloading.
- **Block** – block the object downloading from the web resource.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

DANGEROUS ACTIVITY DETECTED IN THE SYSTEM

When Proactive Defense detects dangerous application activity on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.
- Full name of the file of the process that initiated the dangerous activity and a path to it.
- Possible responses:
    - **Quarantine** – shuts down the process and places the executable file to quarantine. When you place an object in Quarantine, it is moved, not copied. Files in Quarantine are saved in a special format and are not dangerous.

      When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

      > If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after quarantining the file.

    - **Terminate** – shuts down the process.
    - **Allow** – allows the process to execute.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when detecting it.

INVADER DETECTED

When Proactive Defense detects one process attempting to inject into another on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.
- Full name of the file of the process that initiated the implementation attempt and a path to it.

- Possible responses:
  - **Terminate** – completely shuts down the process attempting to inject.
  - **Block** – blocks invaders.
  - **Skip** – takes no actions; simply records information about it in a report.

To apply the selected action to all objects of the same status detected in the current session of protection component or a task operation, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

If you are sure that this action is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when that process attempts to inject into another process.

For example, you use an automatic keyboard layout toggler. Kaspersky Anti-Virus identifies the actions of those programs as dangerous, since attempts to implement in other processes as used by these programs are typical of several malicious programs (for example, password interceptors, etc.).

HIDDEN PROCESS DETECTED

When Proactive Defense detects a hidden process on your system, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com, where you can find detailed information on the type of threat detected.
- Full name of the hidden process file and a path to it.
- Possible responses:
  - **Quarantine** – place the process' executable file to quarantine. When you place an object in Quarantine, it is moved, not copied. Files in Quarantine are saved in a special format and are not dangerous.

    When you scan Quarantine later with updated threat signatures, the status of the object could change. For example, the object may be identified as infected and can be processed using an updated database. Otherwise, the object could be assigned the *not infected* status, and then restored.

    > If a file is quarantined manually and after a subsequent scan turns out to be uninfected, its status will not change to *OK* immediately after the scan. This will only occur if the scan took place after a certain amount of time (at least three days) after file quarantine.

  - **Terminate** – shuts down the process.
  - **Allow** – allows the process to execute.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

If you are sure that the program detected is not dangerous, we recommend adding it to the trusted zone to avoid Kaspersky Anti-Virus making repeat false positives when detecting it.

ATTEMPT TO ACCESS THE SYSTEM REGISTRY DETECTED

When Proactive Defense detects an attempt to access system registry keys, a special notification pops up containing:

- The registry key being accessed.

- Full name of the file of the process that initiated the attempt to access the registry keys and a path to it.
- Possible responses:
  - **Allow** – allows to execute the dangerous action once;
  - **Deny** – blocks the dangerous action once.

To perform the action you have selected automatically every time this activity is initiated on your computer, check the ☑ **Create a rule** box.

If you are sure that any activity by the application that attempted to access system registry keys is not dangerous, add the application to the trusted application list.

ATTEMPT TO REDIRECT CALLING OF SYSTEM FUNCTIONS DETECTED

When Proactive Defense detects attempts to imbed code into the Microsoft Windows operating system kernel to modify the address for calling system functions, a special notification pops up.

The notification's purpose is to inform the user, since such a behavior may be caused by hidden malicious programs or an unknown virus in the system.

In this situation, we recommend you to update the application databases and run the full scan.

NETWORK ACTIVITY OF AN APPLICATION DETECTED

If the Training Mode is enabled for Anti-Hacker, each time an application attempts to establish a network connection that has no matching rule yet, a special notification appears on the screen.

The notification contains:

- *Activity description* – name of the application and general features of the connection it initiates. Generally, the connection type, local port from which it is being initiated, remote port, and address being connected to are given. To obtain detailed information on the connection, the process that initiated it, and the developer of the application, click the **Details** link.
- *Action* – series of operations that Anti-Hacker component should perform regarding the network activity detected.

Carefully review the information on network activity and only then select actions for Anti-Hacker. We recommend that you use these tips when making a decision:

1. Before doing anything else, decide whether to allow or block the network activity. It is possible that in this situation a set of rules already created for this application or packet will help you (assuming that such have been created).
2. Then decide whether to perform this action once or perform it automatically every time this activity is detected.

➡ *To perform the action once,*

uncheck the ☑ **Create a rule** box and select the required action – **Allow** or **Block**.

➡ *To perform selected action automatically every time this activity is initiated on your computer, please do the following:*

1. Make sure that the ☑ **Create a rule** box is checked.

2. Select the type of activity that you want the action to apply to from the dropdown list:

   - **Any activity** – any network activity initiated by this application.
   - **Custom** – specific activity that you will have to define in the rule creation window.
   - **<Template>** – name of the template that includes the set of rules typical of the network activity of the application. This activity type appears on the list if Kaspersky Anti-Virus includes an appropriate template for the application that has initiated the network activity. In such a case, you will not have to customize what activity to allow or block. Use the template and a set of rules for the application will be created automatically.

3. Select a necessary action – **Allow** or **Block**.

Remember that the rule created will be used only when all of the connection parameters match it. This rule will not apply to a connection established from a different local port, for example.

If you do not want to receive notifications from Anti-Hacker, when applications attempt to establish network connections, use the **Turn off Training mode** link. After this, Anti-Hacker will switch to **Minimum protection** mode, which allows all network connections except those that are clearly banned by the rules.

NETWORK ACTIVITY OF A MODIFIED EXECUTABLE FILE DETECTED

If Anti-Hacker detects network activity initiated by the modified executable file of a program that has been started by the user, a special notification will be displayed. A file is considered modified if it has been updated, or infected by a malicious program.

The notification contains:

- *Information about the program that has initiated network activity* – name and ID of the process, as well as the program manufacturer and version number.
- *Action* – series of operations that Kaspersky Anti-Virus should perform regarding the network activity detected.

You are offered to select one of the following actions on the object:

- **Allow** – information about the modified executable file will be updated within the existing rule for application. Further, its network activity will be allowed automatically.
- **Deny** – network activity will be denied once.

NEW NETWORK DETECTED

Every time your computer connects to a new zone (i.e. network), a special notification will pop up.

The upper portion of the notification contains a brief description of the network, specifying the IP address and subnet mask.

The bottom part of the window requests you to assign a status to the zone, and network activity will be allowed based on that status:

- **Internet in Stealth Mode (block external access to computer)**. This feature only allows network activity that the user or an allowed application initiates. This actually means that your computer becomes invisible to its surroundings. This mode does not affect your computer's performance on the Internet.

- **Internet (block file and printer sharing)**. A high-risk network in which your computer is in danger of any possible type of threat. It is recommended to select this status for networks not protected by any anti-virus applications, firewalls, filters etc. When you select this status, the program ensures maximum security for this zone.
- **Local network (allow access to files and printers)**. This status is recommended for zones with an average risk factor (for example, corporate LANs).
- **Trusted network (allow any network activity)**. It is only recommended to apply this status to zones that in your opinion are absolutely safe where your computer is not subject to attacks and attempts to gain access to your data.

It is not recommended to use the Stealth Mode if the computer is being used as a server (for example, mail server or HTTP server). Otherwise, the computers that connect to the server will not see it in the network.

PHISHING ATTACK DETECTED

Every time Kaspersky Anti-Virus detects a phishing attack, a special notification will pop up.

The notification will contain:

- The name of the threat (*phishing attack*) as a link to the Kaspersky Lab's Virus Encyclopedia with a detailed overview of the threat.
- Phishing website address.
- Possible responses:
  - **Allow** – continues phishing site downloading.
  - **Block** – blocks phishing site downloading.

To apply the selected action to all objects with the same status detected in the current session of the protection component or the task, check the ☑ **Apply to all** box. The current session is the time from when the component is started until it is disabled or the application is restarted, or the time from beginning a virus scan until it is complete.

AUTODIAL ATTEMPT DETECTED

When Anti-Spy detects dial attempts to certain numbers, a special notification pops up containing:

- The name of the threat as it is listed in the Kaspersky Lab Virus Encyclopedia. The name of the threat is given as a link to www.viruslist.com where you can find detailed information on the type of threat detected.
- Full filename of the process that has initiated the dial attempt, and the path to it.
- Information on the phone number being called by the dialer.
- Possible responses:
  - **Allow** – allows dialing to the specified number and establishing the network connection;
  - **Block** – blocks dialing to the specified number;
  - **Add to trusted numbers** – add the number to the list of trusted numbers. This option may be used if you have authorized the call to the specified number in order to avoid the application repeating false positives when dialing the number.

INVALID CERTIFICATE DETECTED

Security check for the connection via SSL protocol is performed using the installed certificate. If an invalid certificate is detected when the connection to the server is attempted (for example, if the certificate is replaced by an intruder), a notification will be displayed on the screen.

The notification will contain the information about possible causes of the error, as well as the remote port and the address. You will be prompted to decide if the connection with an invalid certificate should be continued:

- **Accept certificate** – continue connection with the website;
- **Reject certificate** – interrupt connection with the website;
- **View certificate** – view information about the certificate.

WORKING WITH THE APPLICATION FROM THE COMMAND LINE

You can work with Kaspersky Anti-Virus from the command line.

Command line syntax:

```
avp.com <command> [options]
```

You must access the application from the command line from the Kaspersky Anti-Virus installation folder, or by specifying the full path to avp.com.

The following commands can be used as a <command>:

- **HELP –** help with command syntax and list of commands.
- **SCAN –** scanning of objects for malware.
- **UPDATE –** starts the application update.
- **ROLLBACK –** rolls back to the last Kaspersky Anti-Virus update made (the command can only be executed if the password assigned via the application interface is entered).
- **START –** starts a component or a task.
- **STOP –** stops a component or a task (the command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered).
- **STATUS –** displays the current component or task status on screen.
- **STATISTICS –** displays statistics for the component or task on screen.
- **EXPORT –** exports application protection settings.
- **IMPORT –** imports application protection settings (the command can only be executed if the password assigned via the Kaspersky Anti-Virus interface is entered).
- **ACTIVATE –** activates Kaspersky Anti-Virus via Internet using an activation code.
- **ADDKEY –** activates the application using a key file (the command can only be executed if the password assigned via the application interface is entered).
- **RESTORE –** restores a file from quarantine.
- **EXIT –** closes the application (the command can only be executed if the password assigned via the application interface is entered).
- **TRACE –** obtains a trace file.

Each command requires its own specific set of parameters.

IN THIS SECTION

VIEWING HELP

Use this command to view the application command line syntax:

```
avp.com [ /? | HELP ]
```

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

```
avp.com <command> /?
avp.com HELP <command>
```

VIRUS SCAN

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

```
avp.com SCAN [<object scanned>] [<action>] [<file types>] [<exclusions>] [<report
settings>] [<advanced settings>]
```

To scan objects, you can also use the tasks created in the application by starting the one you need from the command line. The task will be run with the settings specified in Kaspersky Anti-Virus interface.

Settings description:

<object to scan> – this parameter gives the list of objects that will be scanned for malicious code. The parameter may include several space-separated values from the list provided:

- **<files>** – list of paths to the files and / or folders to be scanned. You can enter an absolute or relative path to the file. Items on the list are separated by a space. Comments:
  - if the object name contains a space, it must be placed in quotation marks;
  - if reference is made to a specific folder, all files in this folder are scanned.
- **/ALL** – full computer scan.
- **/MEMORY** – RAM objects.
- **/STARTUP** – startup objects.
- **/MAIL** – mail databases.
- **/REMDRIVES** – all removable drives.
- **/FIXDRIVES** – all local drives.
- **/NETDRIVES** – all network drives.
- **/QUARANTINE** – quarantined objects.
- **/@:<filelist.lst>** – path to a file containing a list of objects and catalogs to be scanned. The file should be in text format and each scan object must be listed on a separate line. You can enter an absolute or relative path to the file. The path must be placed in quotation marks even if it contains a space.

<action> – this parameter determines what action will be taken with malicious objects detected during the scan. If this parameter has not been defined, the default action is the one with the value for **/i2**. The following values are possible:

- **/i0** – take no action on the object; simply record information about it in the report.
- **/i1** – treat infected objects and if disinfection is impossible, skip.
- **/i2** – treat infected objects, and if disinfection fails, delete. Do not delete infected objects from compound objects. Delete infected compound objects with executable headers (.sfx archives). This is the default setting.
- **/i3** – treat infected objects and if disinfection fails, delete. Delete all compound objects completely if infected parts cannot be deleted.
- **/i4** – delete infected objects. Delete all compound objects completely if the infected parts cannot be deleted.
- **/i8** – prompt the user for action if an infected object is detected.
- **/i9** – prompt the user for action at the end of the scan.

<file types> – this parameter defines the file types that will be subject to an anti-virus scan. By default, if this parameter is not defined, only infected files by contents will be scanned. The following values are possible:

- **/fe** – scan only infected files by extension.
- **/fi** – scan only infected files by contents.
- **/fa** – scan all files.

<exclusions> – this parameter defines objects that are excluded from the scan. The parameter may include several space-separated values from the list provided.

- **/e:a** – do not scan archives.
- **/e:b** – do not scan email databases.
- **/e:m** – do not scan plain text emails.
- **/e:<mask>** – do not scan objects, which match the mask.
- **/e:<seconds>** – skip objects that are scanned for longer than the time specified in the **<seconds>** parameter.

<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file.

<advanced settings> – settings that define the use of anti-virus scanning technologies and of the settings configuration file:

- **/iChecker=<on|off>** – enable / disable the use of iChecker technology.
- **/iSwift=<on|off>** – enable / disable the use of iSwift technology.
- **/C:<configuration_file_name>** – defines the path to the configuration file that contains the application settings for the scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

Examples:

➧ *Start a scan of memory, startup objects, mail databases, the directories My Documents and Program Files and the file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

➧ *Scan the objects listed in the file object2scan.txt, using the configuration file scan_setting.txt for the job. Use the scan_setting.txt configuration file. When the scan is complete, create a report to log all events:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

A sample configuration file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

UPDATING THE APPLICATION

The syntax for updating the modules of Kaspersky Anti-Virus and application databases from the command line is as follows:

```
avp.com UPDATE [<update_source>] [/APP=<on|off>] [<report_settings>]
[<advanced_settings>]
```

Settings description:

<update_source> – HTTP or FTP server or network folder for downloading updates. If a path is not selected, the update source will be taken from the application update settings.

/APP=<on|off> – enable / disable application modules update.

<report settings> – this parameter determines the format of the report on scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown. The following values are possible:

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file.

<advanced settings> – settings that define the use of the settings configuration file.

/C:<configuration_file_name> – defines the path to the configuration file that contains the application settings for the scan. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

Examples:

➧ *Update application databases and record all events in a report:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➧ *Update the Kaspersky Anti-Virus application modules using the parameters of updateapp.ini configuration file:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

ROLLING BACK THE LAST UPDATE

Command syntax:

```
avp.com ROLLBACK </password=<password>> [<report_settings>]
```

Settings description:

</password=<password>> – a password assigned via the application interface. The ROLLBACK command will not be executed without entering the password.

<report settings> – settings that define the format of the report on scan results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

Example:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

STARTING / STOPPING A PROTECTION COMPONENT OR A TASK

The START command syntax:

```
avp.com START <profile|task_name> [report_settings>]
```

The STOP command syntax:

```
avp.com STOP <profile|task_name> </password=<password>>
```

Settings description:

</password=<password>> – a password assigned via the application interface. The STOP command will not be executed without entering the password.

<report settings> – this parameter determines the format of the report on scan results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown. The following values are possible:

- **/R:<report_file>** – only log important events in this file.
- **/RA:<report_file>** – log all events in this file. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed on screen, and all events are shown.

The **<profile|task_name>** setting can have one of the following values:

- **Protection (RTP)** – all protection components;
- **Anti-Hacker (AH)** – Anti-Hacker;
- **fw** – Firewall;
- **ids** – Intrusion Detection System;
- **Anti-Spam (AS)** – Anti-Spam;
- **Anti-Spy (ASPY)** – Anti-Spy;
- **AdBlocker** – Anti-Banner;
- **antidial** – Anti-Dialer;
- **Behavior_Blocking2** – Proactive Defense;
- **pdm2** – Application Activity Analyzer;
- **regguard2** – Registry Guard;
- **File_Monitoring (FM)** – File Anti-Virus;
- **Web_Monitoring** – Web Anti-Virus;
- **Mail_Monitoring (EM)** – Mail Anti-Virus;
- **Lock_Control (LC)** – Access Control;
- **Device_Locker** – Device Control;
- **Scan_My_Computer** – full computer scan task;
- **Scan_Objects** – objects scan;
- **Scan_Quarantine** – quarantine scan;
- **Scan_Startup (STARTUP)** – startup objects scan;
- **Updater** – update task;
- **Rollback** – updates rollback task.

Components and tasks started from the command line are run with the settings modified through the application's interface.

Examples:

- *To enable File Anti-Virus, type the following in the command prompt:*

```
avp.com START FM
```

- *To stop the full scan task from the command prompt, enter the following:*

```
avp.com STOP SCAN_MY_COMPUTER /password=<your_password>
```

STATISTICS ON A COMPONENT'S OPERATION OR A TASK

The STATUS command syntax:

```
avp.com STATUS <profile|task_name>
```

The STATISTICS command syntax:

```
avp.com STATISTICS <profile|task_name>
```

Settings description:

The **<profile|task_name>** setting can have one of the values specified in the START / STOP command (see page 195).

EXPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com EXPORT <profile|task_name> <file_name>
```

Settings description:

The **<profile|task_name>** setting can have one of the values specified in the START / STOP command (see page 195).

<file_name> – path to the file to which the application settings are being exported. An absolute or a relative path may be specified.

Example:

```
avp.com EXPORT RTP RTP_settings.dat – binary format
avp.com EXPORT FM FM_settings.txt – text format
```

IMPORTING PROTECTION SETTINGS

Command syntax:

```
avp.com IMPORT <file_name> </password=<your_password>>
```

Settings description:

<file_name> – path to the file from which the application settings are being imported. An absolute or a relative path may be specified.

</password=<your_password>> – a password assigned via the application interface.

Example:

```
avp.com IMPORT settings.dat
```

ACTIVATING THE APPLICATION

You can activate Kaspersky Anti-Virus in two ways:

- via the Internet using an activation code (the ACTIVATE command);
- using a key file (the ADDKEY command).

Command syntax:

```
avp.com ACTIVATE <activation_code> </password=<password>>
avp.com ADDKEY <file_name> </password=<password>>
```

Settings description:

<activation_code> – the activation code: xxxxx-xxxxx-xxxxx-xxxxx.

<file_name> – application key file with the .key: xxxxxxxx.key extension.

</password=<password>> – a password assigned via the application interface.

Example:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<password>>
```

RESTORING A FILE FROM QUARANTINE

Command syntax:

```
avp.com RESTORE [/REPLACE] <file_name>
```

Settings description:

/REPLACE – replacement of existing file.

<file_name> – the name of file to restore.

Example:

```
avp.com REPLACE C:\eicar.com
```

CLOSING THE APPLICATION

Command syntax:

```
avp.com EXIT </password=<password>>
```

Settings description:

</password=<password>> – a password assigned via the application interface. The command will not be executed without entering the password.

OBTAINING A TRACE FILE

You might need to create a trace file if you have problems with Kaspersky Anti-Virus. Trace files are useful to troubleshoot problems, and are extensively used by the specialists at Technical Support.

Command syntax:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Settings description:

[on|off] – enable / disable trace file creation.

[file] – output trace to file.

<trace_level> – this value can be an integer from 100 (minimum level, only critical messages) to 600 (maximum level, all messages).

When contacting the Technical Support Service, you should specify the required trace level. If the level is not specified, we recommend setting the value to 500.

Examples:

➧ *To disable trace file creation:*

```
avp.com TRACE file off
```

➧ *Create a trace file with the trace level of 500:*

```
avp.com TRACE file on 500
```

RETURN CODES OF THE COMMAND LINE

The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a specific type of task.

General return codes:

- 0 – operation completed successfully;
- 1 – invalid setting value;
- 2 – unknown error;
- 3 – task completion error;
- 4 – task cancelled.

Virus scan task return codes:

- 101 – all dangerous objects processed;
- 102 – dangerous objects detected.

MODIFYING, REPAIRING, OR REMOVING THE APPLICATION

You can uninstall the application in the following ways:

- using the application setup wizard (see section "Modifying, repairing, and removing the program using the installation wizard" on page 200);
- from the command prompt (see section "Uninstalling the application from the command prompt" on page 202);
- using Kaspersky Administration Kit (please refer to Kaspersky Administration Kit Deployment Guide);
- using Microsoft Windows Server 2000/2003 domain group policies (see section "Uninstalling the application" on page 26).

IN THIS SECTION

MODIFYING, REPAIRING, AND REMOVING THE APPLICATION USING THE INSTALLATION WIZARD

You may find it necessary to repair the application if you have detected errors in its operation after an incorrect configuration or a file corruption.

By changing the components in the application, you can install missing Kaspersky Anti-Virus components or delete those that you do not want nor need.

➧ *To repair or modify missing Kaspersky Anti-Virus components or uninstall the application, please do the following:*

1. Insert the installation CD into your CD/DVD-ROM drive, if you used one to install the application. If you have installed Kaspersky Anti-Virus from a different source (public access folder, folder on your hard drive, etc.), make sure that the application installation package is at the given location and that you have access to it.
2. Select **Start** → **Programs** → **Kaspersky Anti-Virus 6.0 for Windows Workstations MP4** → **Modify, Repair,** or **Remove**.

The installation wizard will then open for the program. Let us take a closer look at the steps that should be taken to repair, modify, or remove the application.

STEP 1. INSTALLATION WELCOME WINDOW

If you have taken all the steps described above and required to repair or modify the application, Kaspersky Anti-Virus installation welcome window will appear. Click the **Next** button to continue.

STEP 2. SELECTING AN OPERATION

At this step, you should select which operation you want to run on the application. You can modify the application components, repair the components that are already installed, or remove several components or the entire application. To execute the operation you need, click the appropriate button. The installation program's response depends on the operation you have selected.

Modifying the application is similar to custom application installation where you can specify which components you want to install, and which ones to delete.

Repairing the application depends on the application components installed. The files will be repaired for all components that have been installed and the **Recommended** security level will be set for each of them.

When removing the application, you can select what data created and used by the application you wish to save on your computer. To delete all Kaspersky Anti-Virus data, select the ◉ **Complete uninstall** option. To save data, select the ◉ **Save application objects** option and specify which objects should not be deleted:

- *Activation information* – key file needed to work with the application.

Application databases - complete set of signatures of dangerous programs, viruses, and other threats current as of the last update.

- *Anti-Spam database* – database used to detect junk email. This database contains detailed information on which mail is spam and which is not.
- *Backup objects* - backup copies of deleted or disinfected objects. We recommend saving these objects, so that they could be restored later.
- *Quarantine objects* - objects that are potentially infected by viruses or modifications of them. These objects contain code that is similar to code of a known virus but it is difficult to determine if they are malicious. It is recommended to save them, since they might prove harmless or could be disinfected after the threat signatures are updated.
- *Application settings* - settings for all application components.
- *iSwift data* - database with information on objects scanned in NTFS. This allows increasing scan speed. Using this database, Kaspersky Anti-Virus only scans the files that have been modified since the last scan.

If a long period of time elapses between uninstalling one version of Kaspersky Anti-Virus and installing another, we do not recommend using the iSwift database saved from a previous installation of the application. A malicious program could penetrate the computer during this period and its effects would not be detected by the database, which could lead to an infection.

To start the operation selected, click the **Next** button. The application will begin copying the necessary files to your computer or deleting the selected components and data.

STEP 3. COMPLETING APPLICATION MODIFICATION, REPAIR, OR REMOVAL

The modification, repair, or removal process is displayed on the screen, after which you will be informed of its completion.

Removing the program generally requires you to restart your computer afterward, since this is necessary to account for modifications to your system. The application will ask if you want to restart your computer. Click the **Yes** button to restart immediately. To restart your computer later, click the **No** button.

REMOVING THE APPLICATION FROM THE COMMAND PROMPT

➧ *To uninstall Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 from the command prompt, execute the following:*

```
msiexec /x <package_name>
```

The installation wizard will open. You may use it to uninstall the application.

➧ *To uninstall the application in non-interactive mode without restarting the computer (the computer should be restarted manually after uninstalling), enter the following:*

```
msiexec /x <package_name> /qn
```

➧ *To uninstall the application in non-interactive mode and then restart the computer, enter the following:*

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

If you opted for password protection against uninstalling the application when you installed the application, you will need to confirm that password when uninstalling the application. Otherwise the application cannot be uninstalled.

➧ *To remove the application when it is password-protected, enter the following:*

`msiexec /x <package_name> KLUNINSTPASSWD=******` – to remove the application in interactive mode;

`msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – to remove the application in non-interactive mode.

MANAGING THE APPLICATION VIA KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit is a system for centrally managing the key administrative tasks in operating a security system for a corporate network, based on the applications included in Kaspersky Anti-Virus Open Space Security. Kaspersky Administration Kit supports all network configurations that use TCP.

The application is intended for administrators of corporate computer networks and employees who are responsible for anti-virus protection in their companies.

Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 is one of the Kaspersky Lab's products that can be administered through its own application interface, the command prompt (these methods are described above herein), or using Kaspersky Administration Kit program (if the computer makes part of a centralized remote administration system).

To manage Kaspersky Anti-Virus via Kaspersky Administration Kit, please do the following:

- deploy *Administration Server* on the network;
- install *Administration Console* on the administrator's workstation (for more details see the Kaspersky Administration Kit Deployment Guide);
- install Kaspersky Anti-Virus and *Network Agent* (included with Kaspersky Administration Kit) on the networked computers. For more details about remote installation of the Kaspersky Anti-Virus installation package on networked computers see Kaspersky Administration Kit Deployment Guide.

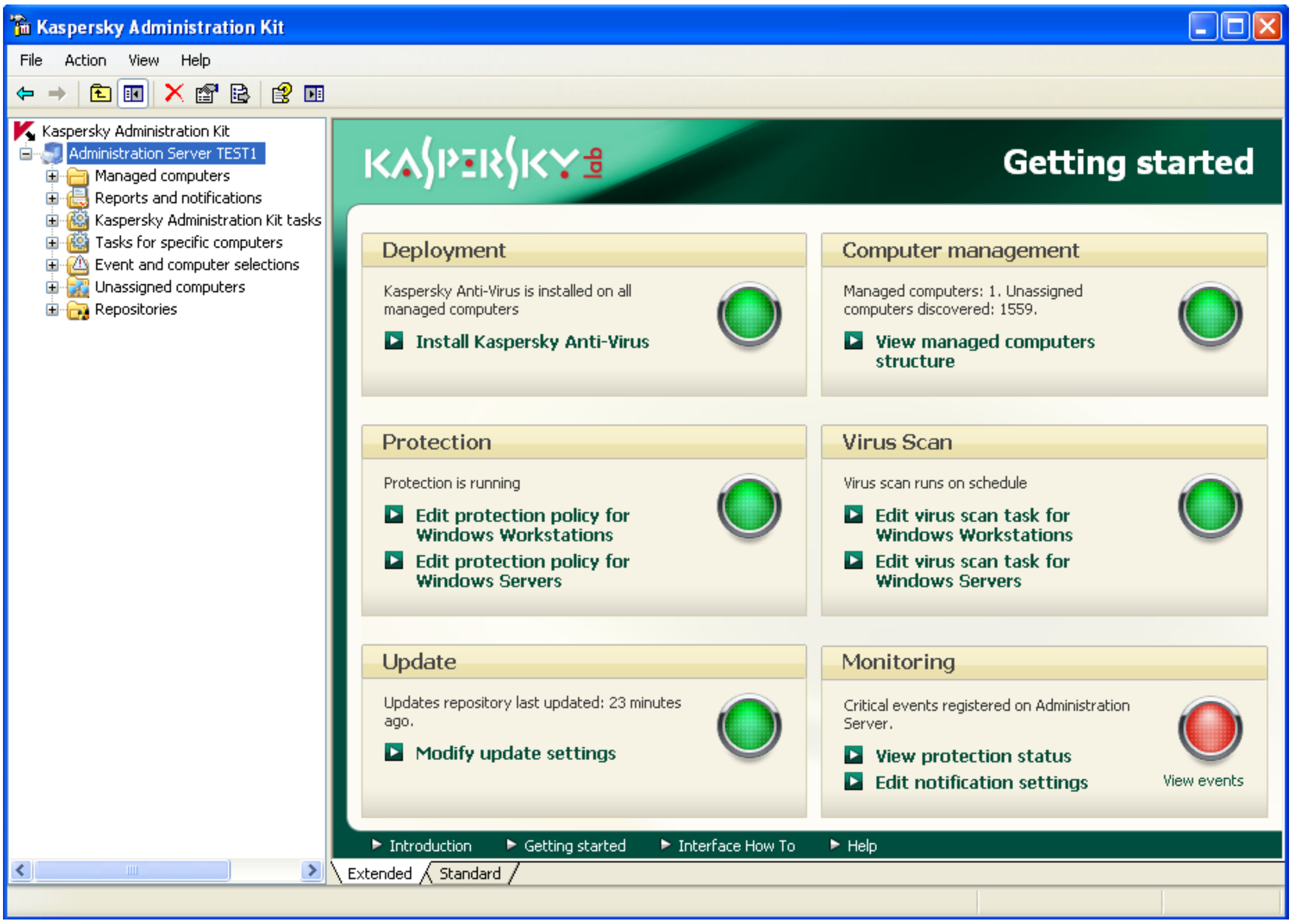
Note that if computers in the network already have the previous version of Kaspersky Anti-Virus installed, you should take the following steps before upgrading to the new version via Kaspersky Administration Kit:

- halt the previous version of the application beforehand (you can do this remotely through Kaspersky Administration Kit);
- close all running applications before beginning installation;
- once installation is complete, restart the operating system on the remote computer.

Before upgrading the Kaspersky Lab administration plug-in through Kaspersky Administration Kit, close Administration Console.

Administration Console (see figure below) allows you to administer the application through Kaspersky Administration Kit. It provides a standard MMC-integrated interface, and allows the administrator to perform the following functions:

- remotely installing and uninstalling Kaspersky Anti-Virus and *Network Agent* on networked computers;
- remotely configuring Kaspersky Anti-Virus on networked computers;
- updating Kaspersky Anti-Virus databases and modules;
- managing licenses for Kaspersky Anti-Virus on networked computers;
- viewing information about the application's operation on client computers.


Kaspersky Administration Kit
File
Action
View
Help
Kaspersky Administration Kit
Administration Server TEST1
Managed computers
Reports and notifications
Kaspersky Administration Kit tasks
Tasks for specific computers
Event and computer selections
Unassigned computers
Repositories
KASPERSKY lab
Getting started
Introduction
Getting started
Interface How To
Help
Extended
Standard

Deployment

Kaspersky Anti-Virus is installed on all managed computers

Install Kaspersky Anti-Virus

Computer management

Managed computers: 1. Unassigned computers discovered: 1559.

View managed computers structure

Protection

Protection is running

Edit protection policy for Windows Workstations

Edit protection policy for Windows Servers

Virus Scan

Virus scan runs on schedule

Edit virus scan task for Windows Workstations

Edit virus scan task for Windows Servers

Update

Updates repository last updated: 23 minutes ago.

Modify update settings

Monitoring

Critical events registered on Administration Server.

View protection status

Edit notification settings

View events

Figure 12. Kaspersky Administration Kit Administration Console

The appearance of the Kaspersky Administration Kit main window may vary depending on the operating system of the computer you are using.

When working via Kaspersky Administration Kit, the application is administered by policy settings, task settings, and application settings set by the administrator.

Named actions taken by the application are referred to as *tasks*. Based on the functions they perform, tasks are divided by *types*: virus scan tasks, application update tasks, update rollbacks, and key file installation tasks.

Each task has a collection of settings for the application that are used when it is executed. The task settings for the application that are common to all types of tasks are the *application settings*. Application settings that are specific to a task type form *task settings*. Application settings and task settings do not overlap.

The key feature of centralized administration is grouping remote computers on the network and managing them by creating and configuring group policies.

Policy is a collection of application settings for a group, as well as a collection of restrictions on re-editing those settings when setting up the application or tasks on an individual client computer. A policy includes settings for configuring all the features of the application, with the exception of settings that are customized for specific instances of a task. Schedule settings are an example.

Thus, policies include the following settings:

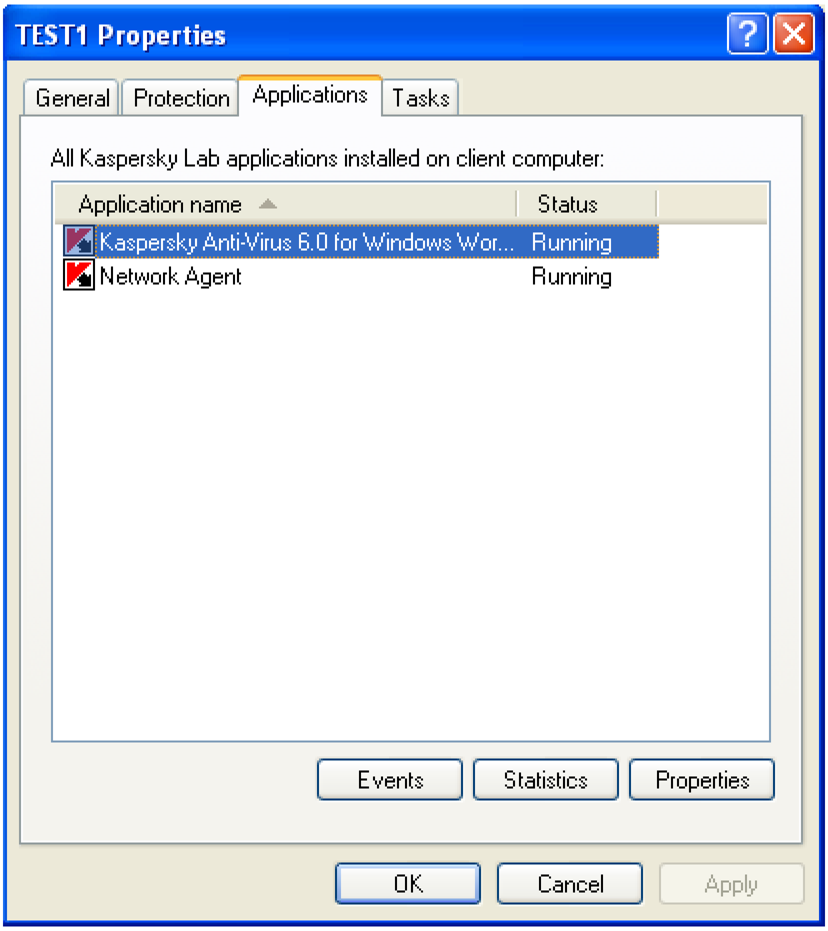
- Settings common to all tasks (application settings);
- Settings common to all instances of a single task type (primarily task settings).

This means that a policy for Kaspersky Anti-Virus, the tasks for which include virus protection and scan tasks, includes all the necessary settings for configuring the application when executing both types of tasks but not, for example, a schedule for running those tasks or settings that define the scan scope.

IN THIS SECTION

MANAGING THE APPLICATION

Kaspersky Administration Kit gives you the opportunity to remotely start and stop Kaspersky Anti-Virus on individual client computers, as well as modifying general settings for the application, such as enabling/disabling computer protection, modifying settings for Backup and Quarantine and reporting.



All Kaspersky Lab applications installed on client computer:

Application name	Status
Kaspersky Anti-Virus 6.0 for Windows Wor...	Running
Network Agent	Running

*Figure 13. Client computer properties window. The **Applications** tab*

To manage the application, please do the following:

1. Open Kaspersky Administration Kit Administration Console.
2. Select the **Managed computers** folder with the name of the group that includes the client computer.

3. In the selected group, open the **Client computers** folder and select the computer for which you need to modify application settings.

4. Select the **Properties** command from the context menu or the corresponding item from the **Action** menu to open the client computer properties window.

5. The **Applications** tab on the properties window of the client computer displays the complete list of Kaspersky Lab applications installed on the client computer. Select **Kaspersky Anti-Virus 6.0 for Windows Workstations MP4** from the list of applications.

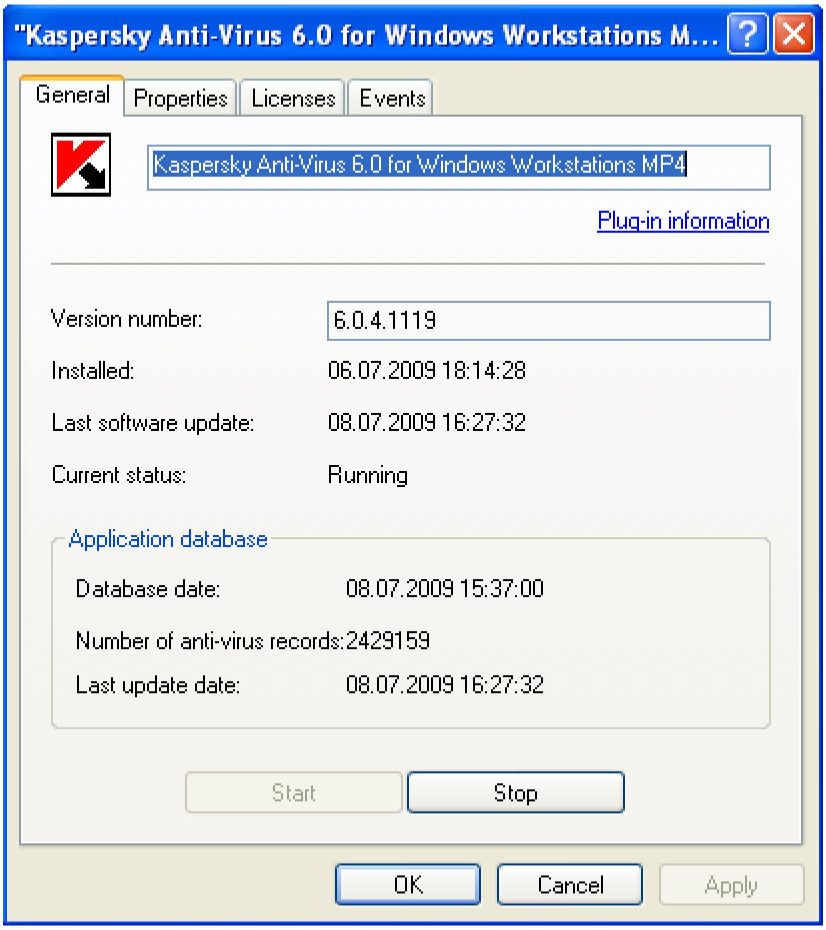
   There are controls under the list of applications that you can use to:

   - view the list of events in application operation that have occurred on the client computer and have been recorded on the Administration Server;
   - view current statistics on application operation;
   - modify application settings (see page 207).

STARTING AND STOPPING THE APPLICATION

Kaspersky Anti-Virus 6.0 is installed and started on remote client computers from the application properties window (see figure below).

In the top part of the window, you will find the name of the application installed, information on the version, the installation date, its status (whether the application is running or stopped on the local computer), and information about the status of the threat signature database.



Kaspersky Anti-Virus 6.0 for Windows Workstations MP4

Version number: 6.0.4.1119

Installed: 06.07.2009 18:14:28

Last software update: 08.07.2009 16:27:32

Current status: Running

Application database

Database date: 08.07.2009 15:37:00

Number of anti-virus records: 2429159

Last update date: 08.07.2009 16:27:32

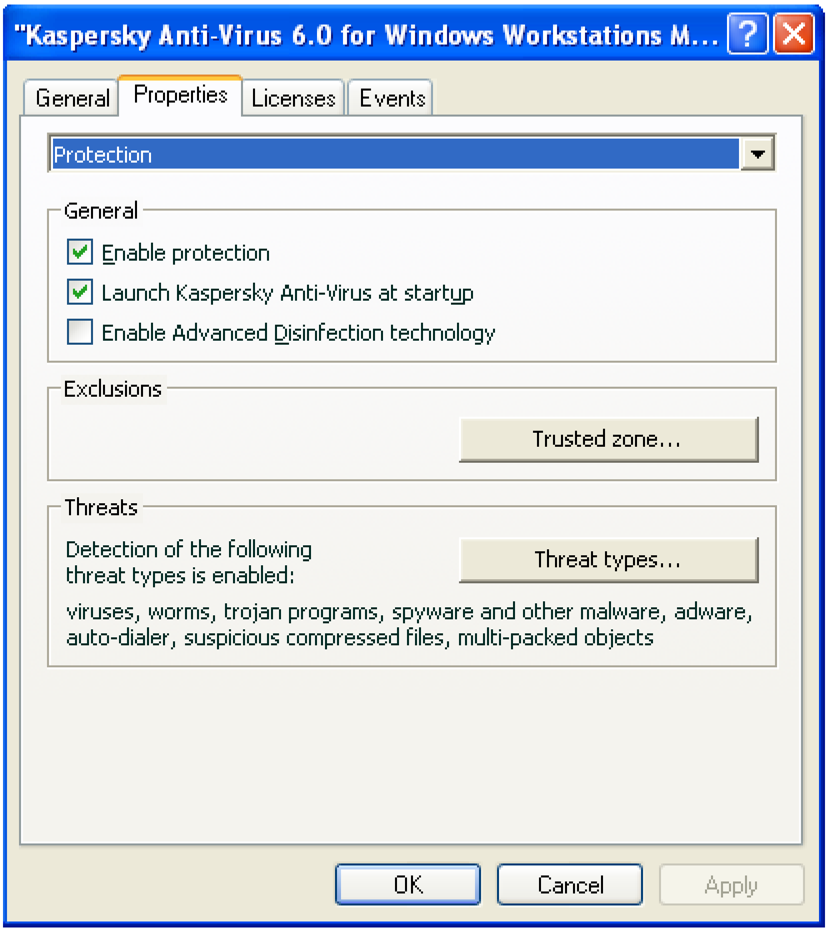
*Figure 14. Application properties window. The **General** tab*

To stop or start the application on a remote computer, please do the following:

1. Open the properties window for the client computer (see page 205) on the **Applications** tab.
2. Select **Kaspersky Anti-Virus 6.0 for Windows Workstations MP4** from the list of applications and click the **Properties** button.
3. In the application properties window that will open, on the **General** tab, click the **Stop** button to stop the application or the **Start** button to start it.

CONFIGURING APPLICATION SETTINGS

You can view and edit application settings in the application properties window on the **Properties** tab (see figure below). The other tabs are standard for the Kaspersky Administration Kit application and are covered in more details in Reference Guide.



Protection

General

☑ Enable protection

☑ Launch Kaspersky Anti-Virus at startup

☐ Enable Advanced Disinfection technology

Exclusions

Trusted zone...

Threats

Detection of the following threat types is enabled:

Threat types...

viruses, worms, trojan programs, spyware and other malware, adware, auto-dialer, suspicious compressed files, multi-packed objects

*Figure 15. Application properties window. The **Properties** tab*

If for the application a policy has been created (see page 242) that prevents some settings from being remodified, they will be unchangeable when configuring the application.

To view and edit the application settings, please do the following:

1. Open the properties window for the client computer (see page 205) on the **Applications** tab.
2. Select **Kaspersky Anti-Virus 6.0 for Windows Workstations MP4** from the list of applications and click the **Properties** button.

3. In the application properties window that will open, on the **Properties** tab you can edit the general settings of Kaspersky Anti-Virus, storage and reporting settings, and network settings. To do so, select the required value from the dropdown menu in the top part of the window, and edit the settings.

SEE ALSO

Enabling / disabling computer protection 144

Launching the application at the operating system startup 145

Selecting detectable threat categories 146

Creating a trusted zone 146

Configuring notification by email 161

Configuring reports 164

Configuring quarantine and backup 166

Configuring specific settings 209

Creating a list of ports to be monitored 166

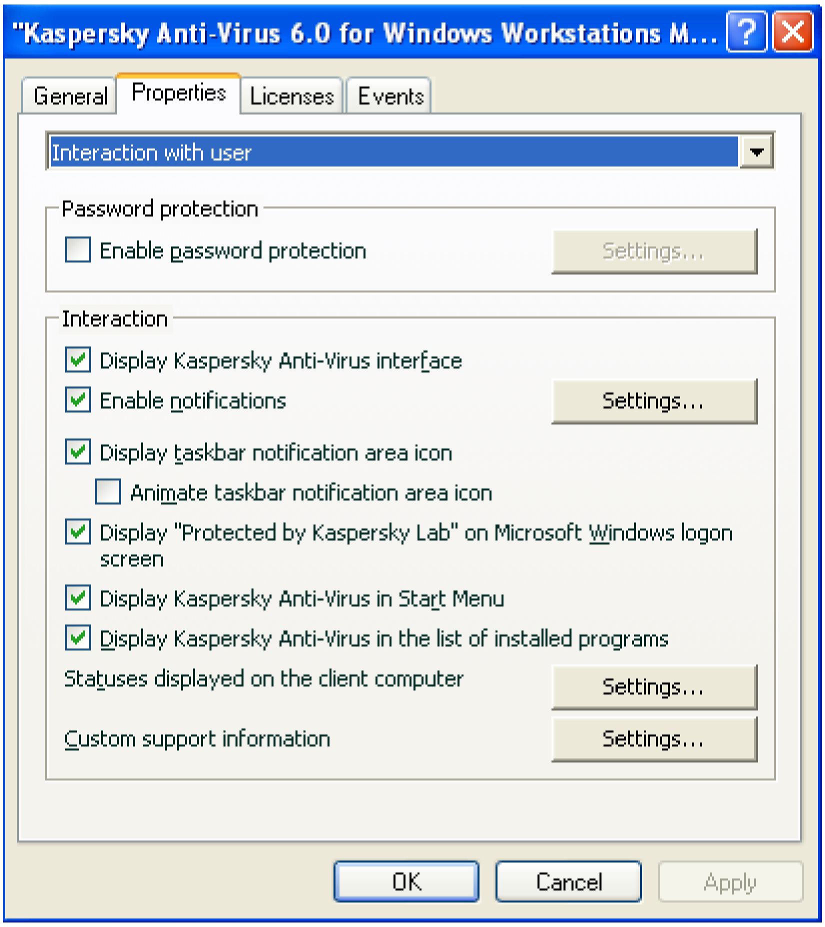
Scanning encrypted connections 167

Creating an exclusion rule 147

Additional exclusion settings 148

CONFIGURING SPECIFIC SETTINGS

When administering Kaspersky Anti-Virus through Kaspersky Administration Kit, you can enable/disable interactivity, configure the appearance of the application, and edit information on Technical Support. These settings can be edited in the application properties window (see figure below).



Interaction with user

Password protection

□ Enable password protection — Settings...

Interaction

☑ Display Kaspersky Anti-Virus interface

☑ Enable notifications — Settings...

☑ Display taskbar notification area icon

□ Animate taskbar notification area icon

☑ Display "Protected by Kaspersky Lab" on Microsoft Windows logon screen

☑ Display Kaspersky Anti-Virus in Start Menu

☑ Display Kaspersky Anti-Virus in the list of installed programs

Statuses displayed on the client computer — Settings...

Custom support information — Settings...

Figure 16. Application properties window. Configuring specific settings

In the **Interaction** section, you can specify the settings for user's interaction with Kaspersky Anti-Virus interface:

- *Displaying application's interface on a remote computer*. If the ☑ **Display Kaspersky Anti-Virus interface** box is checked, a user that works on a remote computer, will see the Kaspersky Anti-Virus icon and pop-up messages, and will have a possibility to make decisions of further actions in notification windows informing about an event. To disable the interactive mode of application's operation, uncheck the box.

- *Event notification*. You can also configure the parameters of notifications about events in application's operation (for example, dangerous object detection). To do this, check the ☑ **Enable notifications** box and click the **Settings** button.

- *Displaying application icon in the taskbar notification area and its animation*. If the ☑ **Display taskbar notification area icon** is checked, a user who works on a remote computer will be able to see the Kaspersky Anti-Virus icon. Depending on the operation being performed by the application, the application icon in the system tray will change. By default, the application icon is animated. In this case, it only displays the protection status of your computer: if the protection is enabled, the icon is in full color; if the protection is paused or disabled, the icon turns grey.

- *Displaying "Protected by Kaspersky Lab" on Microsoft Windows logon screen*. This indicator appears by default in the top right corner of the screen when Kaspersky Anti-Virus loads. It informs you that your computer is protected from any type of threats.

> If the application is installed on a computer running under Microsoft Windows Vista, this option will be unavailable.

- *Displaying the application in Start Menu*. If the ☑ **Display Kaspersky Anti-Virus in Start Menu** is unchecked, a user who works on a remote computer will not be able to see the application in the **Start** menu.

- *Displaying in the list of installed programs*. If the ☑ **Display Kaspersky Anti-Virus in the list of installed programs** box is unchecked, a user who works on a remote computer will not be able to see the application in the list of installed programs.

Besides, you can specify application statuses, which should not be displayed in the main window of Kaspersky Anti-Virus. To do this, in the **Statuses displayed on the client computer** section, click the **Settings** button and check ☑ the security statuses needed in the window that will open. You can specify the monitoring periods of application databases in the same window.

In this window, you can edit information on user technical support that is provided in the **Support info** section of the Kaspersky Anti-Virus **Support** window on a remote computer. To open this window, click the **Settings** button in the **Custom support information** section.

> If for the application a policy has been created (see page 242) that prevents some settings from being remodified, they will be unchangeable when configuring the application.

➡ *To view and edit the application's advanced settings, please do the following:*

1. Open the client computer properties window (see page 205) on the **Applications** tab.

2. Select **Kaspersky Anti-Virus 6.0 for Windows Workstations MP4** from the list of applications and click the **Properties** button.

3. In the application properties window that will open, on the **Properties** tab, select the **Interaction with user** item from the dropdown list, and edit the settings.

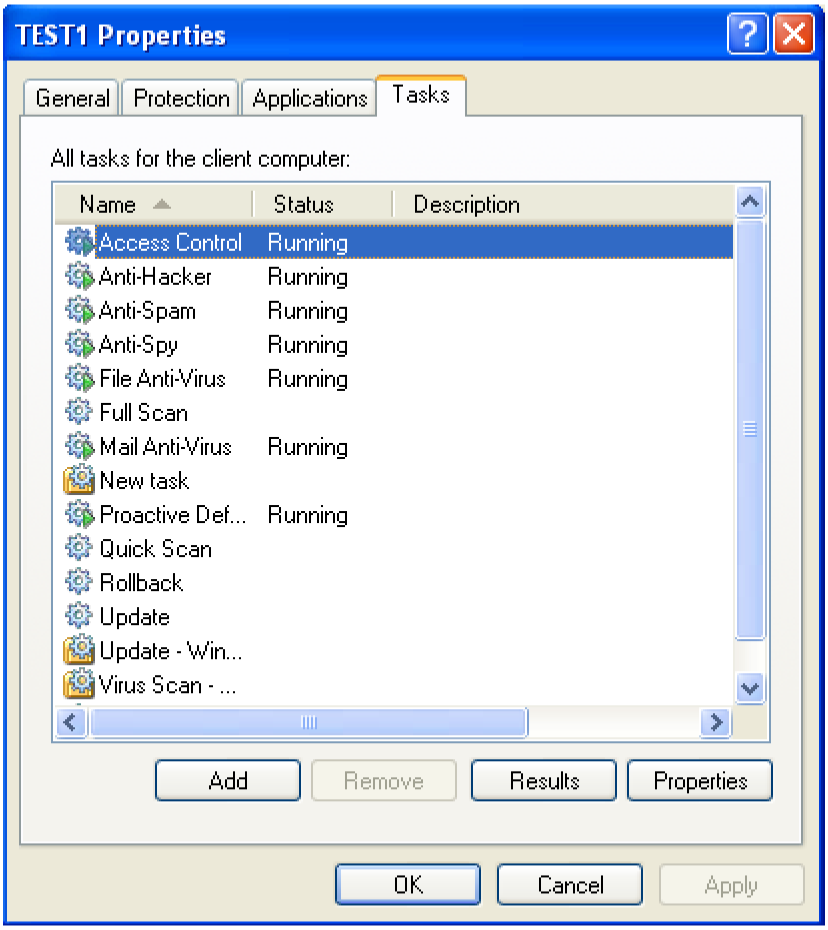
MANAGING TASKS

This section includes information on managing tasks for Kaspersky Anti-Virus. For more details on managing tasks via Kaspersky Administration Kit, consult the Administrator Guide for that product.

A list of system tasks is created for each networked computer when the application is being installed. This list includes protection tasks (File Anti-Virus, Web Anti-Virus, Mail Anti-Virus, Proactive Defense, Anti-Spy, Anti-Hacker, Anti-Spam, Access Control), a number of virus scan tasks (Full Scan, Quick Scan), and update tasks (database and application module updates and database rollbacks).

> You can manage the schedule for system tasks and edit the settings for them. System tasks cannot be deleted.

You can also create your own tasks (see page 212), such as scan tasks, application updates and update rollbacks, and key file installation tasks.



All tasks for the client computer:

Name	Status	Description
Access Control	Running	
Anti-Hacker	Running	
Anti-Spam	Running	
Anti-Spy	Running	
File Anti-Virus	Running	
Full Scan		
Mail Anti-Virus	Running	
New task		
Proactive Def...	Running	
Quick Scan		
Rollback		
Update		
Update - Win...		
Virus Scan - ...		

Figure 17. Client computer properties window. The ***Tasks*** *tab*

➡ *To open the list of tasks created for a client computer, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. Select the **Managed computers** folder with the name of the group that includes the client computer.
3. In the selected group, open the **Client computers** folder and select the computer for which you need to modify application settings.
4. Select the **Properties** command from the context menu or the corresponding item from the **Action** menu to open the client computer properties window.
5. In the client computer properties window that will open, select the **Tasks** tab. Here you will find the complete list of tasks created for the client computer.

STARTING AND STOPPING TASKS

Tasks are started on the client computer only if the corresponding application is running (see page 206). If the application is stopped, all tasks running will be terminated.

Tasks are started and stopped automatically, according to a schedule, or manually using commands from the context menu and from the View Task Settings window. You can also pause tasks and resume them.

➡ *To start/stop/pause/resume a task manually, please do the following:*

1. Open the client computer properties window (see page 210) on the Tasks tab.

2. Select the required task and open the context menu for it. Select the **Start** item to start the task or the **Stop** item to stop it. You can also use the corresponding items in the **Action** menu.

   > You cannot pause or resume a task from the context menu.

   or

   Select the required task from the list and click the **Properties** button. You can use the buttons on the **General** tab in the task properties window that will open to start, stop, pause, or resume a task.

CREATING TASKS

When working with the application via Kaspersky Administration Kit, you can create the following types of tasks:

- local tasks defined for individual client computers;
- group tasks defined for client computers that belong to administration groups;
- tasks for sets of computers that are defined for computers outside of administration groups;
- Kaspersky Administration Kit tasks are specific tasks for the Update Server: update download tasks, backup tasks, and report sending tasks.

> Computer group tasks are only performed on the selected set of computers. If new client computers are added to a group with computers for which a remote installation task has been created, this task will not run for them. You should create a new task or make appropriate changes to the settings of the existing task.

You can take the following actions on tasks:

- specifying tasks settings;
- monitoring task execution;
- copying and moving tasks from one group to another, and also deleting them using the standard commands **Copy/Paste, Cut/Paste, Delete** from the context menu, or the same commands from the **Action** menu;
- importing and exporting tasks.

Consult the Kaspersky Administration Kit Reference Guide for more information on working with tasks.

➡ *To create a local task, please do the following:*

1. Open the client computer properties window (see page 210) on the **Tasks** tab.
2. Click the **Add** button.
3. The New Task Wizard will then start (see page 213). Please follow its instructions.

➡ *To create a group task, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.

3. In the group you have selected, open the **Group tasks** folder, where you will find all of the tasks created for that group.

4. Open the New Task Wizard by clicking the **Create a new task** link in the taskbar. The specifics of creating group tasks are covered in the Kaspersky Administration Kit Reference Guide.

➡ *To create a task for a group of computers (a Kaspersky Administration Kit task), please do the following:*

1. Open Kaspersky Administration Kit Administration Console.

2. Select the **Tasks for specific computers** folder (**Kaspersky Administration Kit tasks**).

3. Open the New Task Wizard by clicking the **Create a new task** link in the taskbar. The specifics of creating Kaspersky Administration Kit tasks and tasks for groups of computers are covered in the Kaspersky Administration Kit Reference Guide.

LOCAL TASK WIZARD

The Local Task Wizard starts when you select the corresponding commands from the context menu for the client computer or from the properties window for that computer.

This wizard consists of a series of boxes (steps) navigated using the **Back** and **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To cancel the wizard at any stage, use the **Cancel** button.

STEP 1. ENTERING GENERAL DATA ON THE TASK

The first wizard window is introductory: all you enter here is the name of the task (the **Name** field).

STEP 2. SELECTING AN APPLICATION AND TASK TYPE

At this step, you should specify the application for which the task is being created (Kaspersky Anti-Virus 6.0 for Windows Workstations MP4, or Administration Agent). You should also select the task type. The possible tasks for Kaspersky Anti-Virus 6.0 are:

- *Scan for viruses* – task of virus scan of the areas specified by the user.

- *Update* – retrieves and applies update packages for the application.

- *Update Rollback* – rolls back to the latest application update.

- *Key file installation* - installation of a key file for a new license as needed to operate the application.

STEP 3. CONFIGURING THE SELECTED TASK TYPE

Depending on the task type selected at the previous step, the contents of the settings window may vary.

The virus scan tasks require you to specify the action that Kaspersky Anti-Virus will take if it detects a malicious object (see page 123) and requires you to create a list of objects to be scanned (see page 122).

For database and application module update tasks, you should specify the source that will be used to download updates (see page 133). The default update source is the Kaspersky Administration Kit update server.

Update rollback tasks have no specific settings.

For license key installation tasks, specify the path to the key file with the **Browse** button. In order to add a file as a license key for an additional license, check the corresponding ☑ box. The additional license key will take effect when the active license key expires.

Information about the specified license (license number, type, and expiration date) is displayed in the field below.

STEP 4. CONFIGURING A SCHEDULE

After configuring the tasks, you will be offered to configure the automatic task run schedule.

To do so, select the frequency for running the task from the dropdown menu in the schedule settings window and modify the schedule settings in the bottom part of the window.

STEP 5. COMPLETING THE TASK CREATION

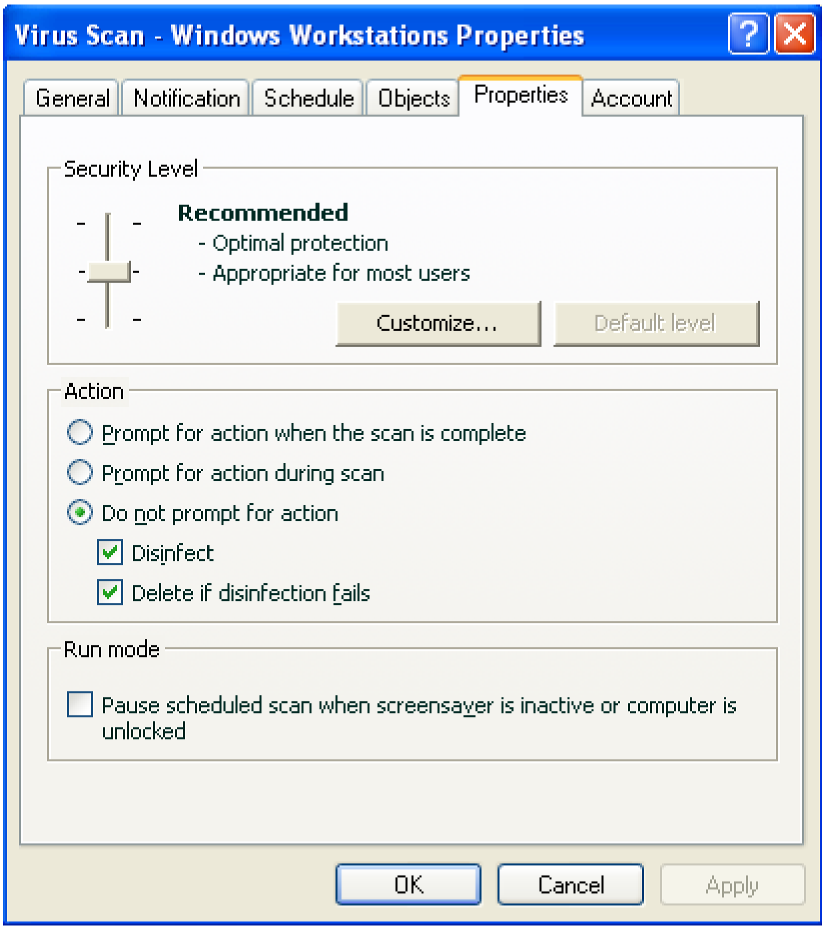
The last window of the wizard will inform you that you have successfully created the task.

CONFIGURING TASKS

Configuring application tasks via the Kaspersky Administration Kit interface is similar to configuring via the local Kaspersky Anti-Virus interface, except for the settings that are edited individually for each user, such as scan tasks run schedule, or settings specific to Kaspersky Administration Kit, such as settings that allow/block managing local scan tasks by the users.

If for the application a policy has been created (see page 242) that prevents some settings from being remodified, they will be unchangeable when configuring the application.

All the tabs, except for the **Properties** tab (see figure below), are standard for the Kaspersky Administration Kit application and are covered more in detail in the Reference Guide. The **Properties** tab contains specific settings for Kaspersky Anti-Virus. The contents of this tab vary depending on the task type selected.



Virus Scan - Windows Workstations Properties

General | Notification | Schedule | Objects | Properties | Account

Security Level

Recommended
- Optimal protection
- Appropriate for most users

Action

○ Prompt for action when the scan is complete
○ Prompt for action during scan
● Do not prompt for action
☑ Disinfect
☑ Delete if disinfection fails

Run mode

□ Pause scheduled scan when screensaver is inactive or computer is unlocked

*Figure 18. Task properties window. The **Properties** tab*

➡ *To view and edit local tasks, please do the following:*

1. Open the client computer properties window (see page 210) on the **Tasks** tab.
2. Select a task from the list and click the **Properties** button. As a result, the task settings window will open.

➡ *To view the group tasks, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.
3. In the group you have selected, open the **Group tasks** folder, where you will find all of the tasks created for that group.
4. Select the required task from the console tree to view and edit its properties.

   The taskbar will display comprehensive information on the task and the links for managing task execution and editing its settings. The specifics of creating group tasks are described in the Kaspersky Administration Kit Reference Guide.

➡ *To view tasks for a group of computers (a Kaspersky Administration Kit task), please do the following:*

1. Open Kaspersky Administration Kit Administration Console.

2. Select the **Tasks for specific computers** folder (**Kaspersky Administration Kit tasks**).

3. Select the required task from the console tree to view and edit its properties.

   The taskbar will display comprehensive information on the task and the links for managing task execution and editing its settings. The specifics of Kaspersky Administration Kit tasks and tasks for sets of computers can be found in the Kaspersky Administration Kit Reference Guide.

MANAGING POLICIES

Setting up policies allows you to apply universal application and task settings to client computers that belong to a single administration group.

This section includes information on creating and configuring policies for Kaspersky Anti-Virus 6.0 for Windows Workstations MP4. For more details on the concept of managing policies through Kaspersky Administration Kit, see the Administrator Guide for the application.

When creating and configuring a policy, you can fully or partially block settings from being edited in policies for nested groups, task settings, and application settings. To do so, click the 🔓 button. It should change to 🔒 for settings that are locked.

➡ *To open the list of policies for Kaspersky Anti-Virus, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.

2. Select the **Managed computers** folder with the name of the group that includes the client computer.

3. In the group you have selected, open the **Policies** folder, where you will find all of the policies created for that group.

CREATING POLICIES

When working with Kaspersky Anti-Virus via Kaspersky Administration Kit, you may create the following types of policies:

You can take the following actions on policies:

- configuring policies;

- copying and moving policies from one group to another, and also deleting them using the standard commands **Copy/Paste, Cut/Paste, Delete** from the context menu, or the same commands from the **Action** menu;

- importing and exporting policy settings.

Working with policies is covered in more details in the Kaspersky Administration Kit Reference Guide.

➡ *To create a policy, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.

2. In the **Managed computers** folder, open the folder with the name of the required group.

3. In the group you have selected, open the **Policies** folder, where you will find all of the policies created for that group.

4. Open the New Task Wizard by clicking the **Create a new policy** link in the taskbar.

5. The New Task Wizard will then start in the window that will open (see page 242): and follow its instructions.

POLICY CREATION WIZARD

The Policy Wizard can be started by selecting the corresponding action from the context menu of the **Policies** folder of the required administration group, or by clicking the link in the results panel (for the **Policies** folders).

This wizard consists of a series of boxes (steps) navigated using the **Back** and **Next** buttons; to close the wizard once it has completed its work, use the **Finish** button. To cancel the wizard at any stage, use the **Cancel** button.

STEP 1. ENTERING GENERAL DATA ON THE POLICY

The first wizard windows are welcome windows. Here you should specify the name of the policy (the **Name** field) and select **Kaspersky Anti-Virus 6.0 for Windows Workstations MP4** from the **Application name** dropdown menu.

If you run the Policy Creation Wizard from the **Policies** node of the taskbar (using the **Create a new Kaspersky Anti-Virus for Windows Workstations MP4 policy**), you will not be able to select an application.

If you want to create a policy based on the settings of an existing policy created for the previous version of the application, check the ☑ **Take settings from existing policy** box and select the policy whose settings should be used in the new policy. To select a policy, click the **Select** button, which will open the list of existing policies that you may use when creating a new one.

STEP 2. SELECTING THE POLICY STATUS

In this window, you will be offered to specify the status of the policy after it is created, selecting one of the following options: active policy, inactive policy, or mobile user policy. Consult the Kaspersky Administration Kit Reference Guide for more details on policy statuses.

Several policies may be created for a single application in a group, but only one of them can be the current (active) policy.

STEP 3. IMPORTING THE APPLICATION SETTINGS

If you have a file with application settings saved earlier, you can specify the path to it using the **Load** button; the wizard windows displayed hereafter will show the imported settings.

STEP 4. CONFIGURING THE PROTECTION

At this step, you can enable/disable or configure protection components that will be used in the policy.

All protection components are enabled by default. To disable any of the components, uncheck the box next to it. To fine-tune a protection component, select it from the list and click the **Configure** button.

STEP 5. CONFIGURING PASSWORD PROTECTION

This wizard window (see figure below) offers you to edit the general application settings: enable/disable self-defense, enable/disable external control of system services, set up password protection for the application, or remove it.

STEP 6. CONFIGURING THE TRUSTED ZONE

In this window of the wizard, you will be offered to configure the trusted zone: add the software used for network administration to the list of trusted applications, and exclude several file types from scan.

STEP 7. CONFIGURING THE INTERACTION WITH THE USER

At this step, you can specify the settings for interaction between the user and Kaspersky Anti-Virus:

- displaying the application's interface on a remote computer;
- notifying the user about events;
- displaying the application icon in the taskbar notification area and animating it;
- displaying "Protected by Kaspersky Lab" on Microsoft Windows logon screen;
- displaying the application in the Start menu;
- displaying the application in the list of applications installed.

STEP 8. COMPLETING THE POLICY CREATION

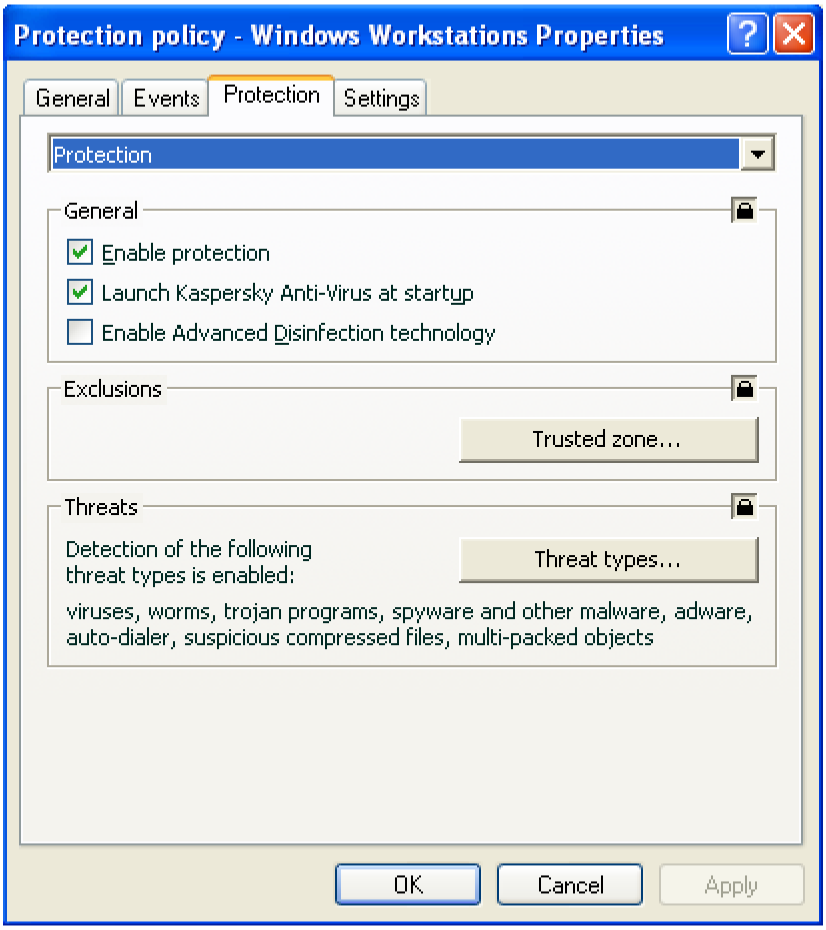
The final window of the wizard will inform you that you have successfully created the policy.

Once the wizard closes, the policy for the application will be added to the **Policies** folder of the corresponding group, becoming visible in the console tree.

You can edit the settings of the policy created and set restrictions on modifying its settings using the 🔓 and 🔒 buttons for each group of settings. If the 🔒 icon is displayed, the client computer user will not be able to edit the settings. If the 🔓 icon is displayed, the user will be able to edit the settings. The policy will be applied to client computers the first time the clients synchronize with the server.

CONFIGURING THE POLICY

At the editing stage, you can modify the policy and block modification of the settings in nested group policies, and in the application and task settings. Policy settings can be edited in the policy properties window (see figure below).



Protection policy - Windows Workstations Properties

General

☑ Enable protection

☑ Launch Kaspersky Anti-Virus at startup

□ Enable Advanced Disinfection technology

Exclusions

Threats

Detection of the following threat types is enabled:

viruses, worms, trojan programs, spyware and other malware, adware, auto-dialer, suspicious compressed files, multi-packed objects

*Figure 19. Policy properties window. The **Protection** tab*

All the tabs, except for the **Protection** and **Settings** tabs, are standard for Kaspersky Administration Kit. They are covered in more details in the Administrator Guide.

Policy settings for Kaspersky Anti-Virus 6.0 include application settings (see page 207) and task settings (see page 214). The **Settings** tab displays the application settings and the **Protection** tab displays the task settings.

To edit settings, select the required value from the dropdown menu in the top part of the window and set it.

➨ *To view and edit policies settings, please do the following:*

1. Open Kaspersky Administration Kit Administration Console.
2. In the **Managed computers** folder, open the folder with the name of the required group.
3. In the group you have selected, open the **Policies** folder, where you will find all of the policies created for that group.
4. Select the required policy from the console tree to view and edit its properties.
5. The taskbar will display comprehensive information on the policy and the links for managing the policy status and editing its settings.

   or

Open the context menu for the policy selected and use the **Properties** item to open the policy settings window of Kaspersky Anti-Virus.

The specifics of working with policies can be found in the Kaspersky Administration Kit Reference Guide.

USING THIRD-PARTY CODE

When creating Kaspersky Anti-Virus, third-party code has been used.

IN THIS SECTION

BOOST-1.30.0 LIBRARY

When creating the application, the Boost-1.30.0 library has been used.

Copyright (C) 2003, Christof Meerwald

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LZMA SDK 4.40, 4.43 LIBRARY

When creating the application, the LZMA SDK 4.40, 4.43 library has been used.

OPENSSL-0.9.8D LIBRARY

When creating the application, OpenSSL-0.9.8d library has been used.

Copyright (C) 1998-2007, The OpenSSL Project

LICENSE

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL

please contact openssl-core@openssl.org.

OpenSSL License

==

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA,

lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution

as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

WINDOWS TEMPLATE LIBRARY 7.5

When creating the application, the Windows Template Library 7.5 has been used.

Copyright (C) 2006, Microsoft Corporation

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce", "reproduction", "derivative works", and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

WINDOWS INSTALLER XML (WIX) TOOLSET 2.0 LIBRARY

When creating the application, the Windows Installer XML (WiX) toolset 2.0 library has been used.

Copyright (C) 2009, Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE

EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZIP-2.31 LIBRARY

When creating the application, the ZIP-2.31 library has been used.

Copyright (C) 1990-2005, Info-ZIP

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 LIBRARY

When creating the application, the ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3 library has been used.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

UNZIP-5.51 LIBRARY

When creating the application, the UNZIP-5.51 library has been used. Copyright (c) 1990-2004 Info-ZIP.

LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 LIBRARY

When creating the application, the LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 library has been used.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following

this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg" (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a

certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

LIBJPEG-6B LIBRARY

When creating the application, the LIBJPEG-6B library has been used.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

============

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code,

not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name

in advertising or publicity relating to this software or products derived from

it. This software may be referred to only as "the Independent JPEG Group's

software".

We specifically permit and encourage the use of this software as the basis of

commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch,

sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead

by the usual distribution terms of the Free Software Foundation; principally,

that you must include source code if you redistribute it. (See the file

ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part

of any program generated from the IJG code, this does not limit you more than

the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has

been removed altogether, and the GIF writer has been simplified to produce

"uncompressed GIFs". This technique does not use the LZW algorithm; the

resulting GIF files are larger than usual, but are readable by all standard

GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of

CompuServe Incorporated. GIF(sm) is a Service Mark property of

CompuServe Incorporated."

LIBUNGIF-4.1.4 LIBRARY

When creating the application, the LIBUNGIF-4.1.4 library has been used.

PCRE-3.0 LIBRARY

When creating the application, the PCRE-3.0 library has been used.

REGEX-3.4A LIBRARY

When creating the application, the regex-3.4a library has been used.

MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 LIBRARY

When creating the application, the MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 library has been used.

MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 LIBRARY

When creating the application, the MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 library has been used.

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

When creating the application, the INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 library has been used.

RSA's MD5 disclaimer

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

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

When creating the application, the CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 library has been used.

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM LIBRARY

When creating the application, the COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum library has been used.

FMT-2002 LIBRARY

When creating the application, the Fmt-2002 library has been used.

EXPAT-1.95.2 LIBRARY

When creating the application, the expat-1.95.2 library has been used.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY

CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,

TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE

SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBNKFM-0.1 LIBRARY

When creating the application, the libnkfm-0.1 has been used.

Copyright (C) 1987, Fujitsu LTD (Itaru ICHIKAWA)

Everyone is permitted to do anything on this program including copying, modifying, improving, as long as you don't try to pretend that you wrote it. i.e., the above copyright notice has to appear in all copies. Binary distribution requires original version messages. You don't have to ask before copying, redistribution or publishing.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE.

PLATFORM INDEPENDENT IMAGE CLASS LIBRARY

When creating the application, the PLATFORM INDEPENDENT IMAGE CLASS library has been used.

Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx)

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

NETWORK KANJI FILTER (PDS VERSION)-2.0.5 LIBRARY

When creating the application, the Network Kanji Filter (PDS Version)-2.0.5 library has been used.

Copyright (C) 1987, Fujitsu LTD. (Itaru ICHIKAWA)

Everyone is permitted to do anything on this program including copying, modifying, improving,

as long as you don't try to pretend that you wrote it. i.e., the above copyright notice has to appear in all copies. Binary distribution requires original version messages. You don't have to ask before copying, redistribution or publishing.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE.

DB-1.85 LIBRARY

When creating the application, the db-1.85 library has been used.

Copyright (C) 1990, 1993, 1994, The Regents of the University of California

----

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

SUCH DAMAGE.

LIBNET-1991, 1993 LIBRARY

When creating the application, the libnet-1991, 1993 library has been used.

Copyright (C) 1991, 1993, The Regents of the University of California

----

This code is derived from software contributed to Berkeley by Berkeley Software Design, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GETOPT-1987, 1993, 1994 LIBRARY

When creating the application, the getopt-1987, 1993, 1994 library has been used.

Copyright (C) 1987, 1993, 1994, The Regents of the University of California

----

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MERGE-1992, 1993 LIBRARY

When creating the application, the merge-1992, 1993 library has been used.

This code is derived from software contributed to Berkeley by Peter McIlroy.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FLEX PARSER (FLEXLEXER)-V. 1993 LIBRARY

When creating the application, the FLEX PARSER (FLEXLEXER)-V. 1993 library has been used.

This code is derived from software contributed to Berkeley by

Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: ``This product includes software developed by the University of California, Berkeley and its contributors'' in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

STRPTIME-1.0 LIBRARY

When creating the application, the strptime-1.0 library has been used.

ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 LIBRARY

When creating the application, the ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 library has been used.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

OUTLOOK2K ADDIN-2002 LIBRARY

When creating the application, the Outlook2K Addin-2002 library has been used.

Copyright (C) 2002, Amit Dey email :amitdey@joymail.com

This code may be used in compiled form in any way you desire. This file may be redistributed unmodified by any means PROVIDING it is not sold for profit without the authors written consent, and providing that this notice and the authors name is included.

This file is provided 'as is' with no expressed or implied warranty. The author accepts no liability if it causes any damage to your computer.

Do expect bugs.

Please let me know of any bugs/mods/improvements.

and I will try to fix/incorporate them into this file.

Enjoy!

STDSTRING- V. 1999 LIBRARY

When creating the application, the STDSTRING- V. 1999 library has been used.

Copyright (C) 1999, Joseph M. O'Leary

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your $30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

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

When creating the application, the T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 library has been used.

NTSERVICE- V. 1997 LIBRARY

When creating the application, the NTSERVICE- V. 1997 library has been used.

SHA-1-1.2 LIBRARY

When creating the application, the SHA-1-1.2 library has been used.

COCOA SAMPLE CODE- V. 18.07.2007 LIBRARY

When creating the application, the Cocoa sample code- v. 18.07.2007 library has been used.

PUTTY SOURCES-25.09.2008 LIBRARY

When creating the application, the PUTTY SOURCES-25.09.2008 library has been used. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified http://www.opensource.org/licenses/ and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

OTHER INFORMATION

Crypto C program library, developed by CryptoEx OOO (http://www.cryptoex.ru), is used to check digital signature.

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

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

GLOSSARY

A

Active license

The license currently used for the operation of a Kaspersky Lab application. The license defines the expiration date for full functionality and the license policy for the application. The application cannot have more than one license with the active status.

Additional license

A license that has been added for the operation of Kaspersky Lab application but has not been activated. The additional license enters into effect when the active license expires.

Administration agent

Kaspersky Administration Kit component that handles interactions between Administration Server and Kaspersky Lab applications installed on a specific network node (a workstation or a server). This component is the same for all Windows applications in the company's product line. There are separate versions of Administration agent for Novell- and Unix-specific applications by Kaspersky Lab.

Archive

File "containing" one or several other objects which can also be archives.

Available updates

A set of updates for Kaspersky Lab application modules including critical updates accumulated over a period of time and changes to the application's architecture.

B

Backup

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

Backup copy

Creating a backup copy of a file before any processing and putting the copy into the backup storage area with the possibility of restoring the file later, for example, to scan it with updated databases.

Backup storage

A special storage folder for copies of Administration Server data created using a backup utility.

Black list of addresses

The list of email addresses which send the messages that should be blocked by Kaspersky Lab application, regardless of their content.

Black list of key files

A database containing information on blacklisted Kaspersky Lab key files whose owners violated the terms of the license agreement and information on key files that were issued but for some reason were not sold or were replaced. A blacklist file is necessary for the operation of Kaspersky Lab applications. File contents is updated together with the databases.

Blocking the object

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

Boot-virus

A virus that infects the boot sectors of a computer's hard drive. The virus forces the system to load it into memory during reboot and to direct control to the virus code instead of the original boot loader code.

C

CLIENT

The program that connects with the server by using a specific service. For example, **Netscape** is a **WWW** client and connects with web servers to download web pages.

COMPRESSED FILE

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

CONTENT FILTERING DATABASES

Databases created by Kaspersky Lab engineers that contain sample spam and terminology typical of spam (words and phrases). The application performs a linguistic analysis of the contents of emails and attachments based on this database. Databases are regularly updated at Kaspersky Lab. This requires administrators to perform updates regularly for the databases used by the application.

D

DANGEROUS OBJECT

Object containing a virus. You are advised not to access these objects, because it may result in an infection of your computer. Once an infected object is detected, we recommend that you disinfect it using one of Kaspersky Lab's applications, or delete it if disinfection is not possible.

DATA FOLDER

The folder containing service folders and databases needed for working with the application. Is the data folder is moved, all of the information that it includes must be saved at the new location.

DATABASE UPDATES

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

DATABASES

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

DELETING AN OBJECT

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

DISINFECTING OBJECTS ON RESTART

A method of processing infected objects that are being used by other applications at the moment of disinfection. Consists of creating a copy of the infected object, disinfecting the copy created, and replacing the original infected object with the disinfected copy after the next system restart.

DISK BOOT SECTOR

A boot sector is a particular area on a computer's hard drive, floppy, or other data storage device. It contains information on the disc's file system and a boot loader program that is responsible for starting the operating system.

There exist a number of viruses that infect boot sectors, which are thus called boot viruses. The Kaspersky Lab application allows to scan boot sectors for viruses and disinfect them if an infection is found.

E

EVENT SEVERITY LEVEL

Description of an event logged during the operation of a Kaspersky Lab's application. There exist four severity levels:

- **Critical event**.
- **Functional failure**.
- **Warning**.
- **Informational message**.

Events of the same type may have different severity levels, depending on the situation when the event occurred.

EXCLUSION

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

F

FALSE ALARM

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

FILE MASK

Representation of a file name and extension using wildcards. The two standard wildcards used in file masks are ***** and **?**, where ***** represents any number of characters and **?** stands for any single character. Using these wildcards, you can represent any file. Note that the name and extension are always separated by a period.

H

HEADER

The information in the beginning of a file or a message, which is comprised of low-level data on file (or message) status and processing. In particular, the email message header contains such data as information about the sender and the recipient, and the date.

HEURISTIC ANALYZER

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

The use of heuristic analyzer detects up to 92% of threats. This mechanism is fairly effective and very rarely leads to false positives.

Files detected by the heuristic analyzer are considered suspicious.

HOST

Computer where the server software is running. One host can run numerous server programs - for example, an FTP server, a mail server, and a Web server can run on the same host. The user uses a client program (such as a Web browser) to access the host. The term "server" is also often used to refer to the computer where server software is running, which blurs the distinction between a server and a host.

In telecommunications, a host is a computer that sends information (such as FTP files, news, or web pages). Within the Internet, hosts are also often referred to as **nodes**.

I

ICHECKER TECHNOLOGY

iChecker is a technology that increases the speed of anti-virus scans by excluding objects that have remain unchanged since their last scan, provided that the scan parameters (the anti-virus database and settings) have not changed. The information for each file is stored in a special database. This technology is used in both real-time protection and on-demand scan modes.

For example, you have an archive scanned by Kaspersky Lab application which has been assigned the not infected status. The next time the application will skip this archive, unless it has been altered or the scan settings have been changed. If you altered the archive content by adding a new object to it, modified the scan settings or updated the anti-virus database, the archive will be re-scanned.

Limitations of **iChecker** technology:

- this technology does not work with large-size files since it is faster to scan a file than check whether it was modified since it had been last scanned;
- the technology supports a limited number of formats (**.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar**).

INCOMPATIBLE APPLICATION

An antivirus application from a third party developer or a Kaspersky Lab application that does not support management through Kaspersky Administration Kit.

INFECTED OBJECT

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

INTERCEPTOR

Subcomponent of the application responsible for scanning specific types of email. The set of interceptors specific to your installation depends on what role or what combination of roles the application is being deployed for.

INTERNET PROTOCOL (IP)

The base protocol for the Internet, used without change since the time of its development in 1974. It performs basic operations in transmitting data from one computer to another and serves as a foundation for higher-level protocols like TCP and UDP. It manages the connection and error processing. Technologies such as NAT and masking make it possible to hide a large number of private networks using a small number of IP addresses (or even one address), which make it possible to respond to the demands of the constantly growing Internet area using the relatively restricted IPv4 address space.

K

KASPERSKY ANTI-VIRUS ADMINISTRATOR

Person who manages the application's operation via the remote centralized administration system of Kaspersky Anti-Virus.

KASPERSKY LAB'S UPDATE SERVERS

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

KEY FILE

File with the **.key** extension, which is your personal "key", necessary for working with Kaspersky Lab application. A key file is included with the product if you have purchased it from Kaspersky Lab distributors, or it is emailed to you if you have purchased the product at eStore.

L

LICENSE VALIDITY PERIOD

Period of time during which you are able to use all of the features of your Kaspersky Lab's application. License validity period generally accounts for one calendar year from the date of its installation. After the license expires, the application will have reduced functionality. You will not be able to update the application databases.

M

MAIL DATABASES

Databases containing emails in a special format and saved on your computer. Each incoming/outgoing email is placed in the mail database after it is received/sent. These databases are scanned during a full computer scan.

Incoming and outgoing emails at the time that they are sent and received are analyzed for viruses in real time if real-time protection is enabled.

MAXIMUM PROTECTION

Security level for your computer corresponding to the most complete protection that an application can provide. At this protection level, all files on the computer, removable storage media, and network drives are scanned for viruses if connected to the computer.

MESSAGE DELETION

Method of processing an email message that contains spam signs, at which the message is physically removed. This method is advised to apply to messages unambiguously containing spam. Before deleting a message, a copy of it is saved in the backup (unless this option is disabled).

MONITORED OBJECT

A file transferred via HTTP, FTP, or SMTP protocols across the firewall and sent to a Kaspersky Lab application to be scanned.

MOVING OBJECTS TO QUARANTINE

A method of processing a potentially infected object by blocking access to the file and moving it from its original location to the Quarantine folder, where the object is saved in encrypted form, which rules out the threat of infection. Quarantined objects can be scanned using updated Anti-Virus databases, analyzed by the administrator, or sent to Kaspersky Lab.

N

NETWORK PORT

TCP and UDP parameter that determines the destination of data packets in IP format that are transmitted to a host over a network and makes it possible for various programs running on a single host to receive data independently of each other. Each program processes data received via certain port (this is sometimes referred to as the program "listening" to that port).

For some common network protocols there are usually standard port numbers (for example, web servers usually receive HTTP requests on TCP port 80); however, generally, a program can use any protocol on any port. Possible values: 1 to 65535.

O

OBJECT DISINFECTION

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

OBSCENE MESSAGE

Email message containing offensive language.

OLE OBJECT

An attached object or an object embedded into another file. Kaspersky Lab application allows to scan OLE objects for viruses. For example, if you insert a Microsoft Office Excel table into a Microsoft Office Word document, the table will be scanned as an OLE object.

ON-DEMAND SCAN

Operating mode of the Kaspersky Lab application that is initiated by the user and can target any files on the computer.

P

POTENTIALLY INFECTABLE OBJECT

An object which, due to its structure or format, can be used by intruders as a "container" to store and distribute a malicious object. As a rule, they are executable files, for example, files with the **.com, .exe, .dll** extensions, etc. The risk of activating any malicious code in such files is fairly high.

POTENTIALLY INFECTED OBJECT

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

PROTECTION STATUS

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

PROTOCOL

Clearly defined and standardized set of rules governing the interaction between a client and a server. Well-known protocols and the services associated with them include HTTP (WWW), FTP, and NNTP (news).

Q

QUARANTINE

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

R

REAL-TIME PROTECTION

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on to the user; objects containing threats or suspected of containing them are processed pursuant to the task settings (they are disinfected, deleted or quarantined).

RECOMMENDED LEVEL

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

RESTORATION

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

S

SCRIPT

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

If real-time protection is enabled, the application will track the scripts launching, intercept them, and scan for viruses. Depending on the results of the scan you can block or allow the execution of a script.

SIMPLE OBJECT

Email body or simple attachments, for example, an executable file. Also see container objects.

SKIPPING OBJECTS

A method of processing in which an object is passed on to the user without any changes. If event logging is enabled for this event type, information about the object detected will be logged in the report.

SOCKS

Proxy server protocol that allows to establish a point-to-point connection between computers in the internal and external networks.

SPAM

Unsolicited mass mailings, most often including advertising messages.

STARTUP OBJECTS

The set of programs needed to start and correctly operate the operating system and software installed on your computer. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which could lead to, for example, blocking your access to the operating system.

STORAGE SCAN

Scanning the email stored on the mail server and the contents of shared folders using the latest version of the database. The scan runs in the background and can be run using a schedule or on demand. All shared folders and mailbox storage are scanned. New viruses may be detected during the scan about which no information was in the database at the time of previous scans.

SUBNET MASK

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

SUSPICIOUS MESSAGE

Message that cannot be unambiguously considered spam, but it seems suspicious when scanned (e.g., certain types of mailings and advertising messages).

SUSPICIOUS OBJECT

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

T

TRAFFIC SCAN

A real-time scan using information from the latest version of the databases for objects transmitted over all protocols (for example, HTTP, FTP, etc.).

TRUSTED PROCESS

Application process whose file operations are not monitored by Kaspersky Lab's application in real-time protection mode. In other words, no objects launched, opened, or saved by the trusted process will be scanned.

U

UNKNOWN VIRUS

A new virus about which there is no information in the databases. Generally unknown viruses are detected by the application in objects using the heuristic analyzer, and those objects are classified as potentially infected.

UPDATE

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

UPDATE PACKAGE

File package for updating the software. It is downloaded from the Internet and installed on your computer.

URGENT UPDATES

Critical updates to Kaspersky Lab application modules.

V

VIRUS ACTIVITY THRESHOLD

The maximum permissible level of a specific type of event over a limited time period that, when exceeded, will be considered excessive virus activity and a threat of a virus outbreak. This feature is significant during virus outbreaks and enables an administrator to react in a timely fashion to threats of virus outbreaks that arise.

VIRUS OUTBREAK

A series of deliberate attempts to infect a computer with a virus.

W

WHITE LIST OF ADDRESSES

The list of email addresses which send the messages that should not be scanned by Kaspersky Lab application.

KASPERSKY LAB

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

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

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

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

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

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

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

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

LICENSE AGREEMENT

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

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

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

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

1.1. **Software** means software including any Updates and related materials.

1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.

1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.

1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, *"You"* further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term *"organization,"* without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.

1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.

1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

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

2. Grant of License

2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:
Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the

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

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

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

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

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

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

3. Activation and Term

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

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

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

3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline.

3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.

3.6. If You have acquired the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.

3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.

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

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

4. Technical Support

The Technical Support described in Clause 2.5 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).
Technical support service: http://support.kaspersky.com

5. Limitations

5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

5.2. You shall not transfer the rights to use the Software to any third party except as set forth in additional agreement.

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

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

5.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

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

5.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don’t have the right to transfer the license or the rights to use the Software to any third party.

6. Limited Warranty and Disclaimer

6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer’s deficiencies and related infringement for which Rightholder’s expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties’ or Your actions or causes beyond Rightholder’s reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.

6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

6.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

6.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.5 of this Agreement.

6.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this Agreement or after the License to use the Software is terminated for any reason.

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

7. Exclusion and Limitation of Liability

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

(INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

8. GNU and Other Third Party Licenses

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

9. Intellectual Property Ownership

9.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

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

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

10. Governing Law; Arbitration

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

11. Period for Bringing Actions

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

12. Entire Agreement; Severability; No Waiver

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

13. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

INDEX