

KASPERSKY LAB

Kaspersky Anti-Virus[®] 5.0 SOS

Administrator's Guide

KASPERSKY ANTI-VIRUS® 5.0
SOS

Administrator's Guide

© Kaspersky Lab
<http://www.kaspersky.com>

Revision date: October, 2006

Contents

CHAPTER 1. KASPERSKY ANTI-VIRUS SOS	7
1.1. Hardware and software system requirements	8
1.2. Distribution kit	9
1.2.1. License Agreement.....	10
1.3. Services for registered users	10
1.4. Conventions.....	11
CHAPTER 2. INSTALLATION AND REMOVAL OF THE APPLICATION	12
2.1. Installing the application	12
2.2. Silent mode installation of the application.....	15
2.3. Removing the application.....	17
CHAPTER 3. APPLICATION MANAGEMENT CONCEPTS	18
3.1. Basic concepts of the administration concept	19
3.2. Local interface	20
3.2.1. System tray icon	20
3.2.2. Right-click menu	20
3.2.3. Main application window: general structure.....	21
3.2.3.1. The <i>Protection</i> tab.....	22
3.2.3.2. The <i>Settings</i> tab.....	23
3.2.3.3. The <i>Support</i> tab	25
3.2.4. Scanning process window.....	26
3.2.5. Help system	27
CHAPTER 4. COMPUTER PROTECTION USING THE DEFAULT SETTINGS	28
4.1. Default settings	28
4.2. Anti-Virus scan levels	29
CHAPTER 5. APPLICATION MANAGEMENT USING THE LOCAL INTERFACE ...	32
5.1. Updating the anti-virus database and application modules	32
5.1.1. When to download updates.....	32
5.1.2. Performing manual update. Downloading updates	33
5.1.3. Configuring updates	34

5.1.3.1. Updating the application modules	37
5.1.3.2. Copying updates to the local folder	38
5.1.3.3. Selecting the updates source	39
5.1.3.4. Proxy server settings configuration	41
5.1.3.5. Selecting anti-virus database type	42
5.2. The on-demand scan mode.....	43
5.2.1. Full computer scan	44
5.2.2. Scanning selected objects.....	46
5.2.3. Configuring on-demand scan.....	48
5.2.3.1. Selecting the scan level	51
5.2.3.2. Actions to be performed with a detected object	54
5.2.4. Scanning archives	56
5.2.5. Scanning removable drives	58
5.3. Processing malicious objects detected.....	59
5.4. User's tasks	63
5.5. Creating list of exclusions.....	64
5.6. Configuring schedule.....	68
5.7. Launching a task under a selected user's account	71
5.8. Additional features.....	72
5.8.1. Quarantine and Backup storage	72
5.8.1.1. Storage setup.....	73
5.8.1.2. Work with Quarantine storage.....	74
5.8.1.3. Working with Backup storage.....	76
5.8.2. Working with reports.....	78
5.8.3. Managing Kaspersky Anti-Virus configuration.....	83
5.8.4. Additional settings.....	83
5.8.5. Configuring prompts for confirmation.....	88
5.8.6. Restricting efficiency of Kaspersky Anti-Virus	89
5.8.7. Working in the administrator's and the user's mode	89
CHAPTER 6. MANAGING THE APPLICATION USING KASPERSKY ADMINISTRATION KIT.....	91
6.1. Managing installation packages.....	91
6.1.1. Creating an installation package	91
6.1.2. Viewing and editing the installation package settings	94
6.2. Managing policies.....	95
6.2.1. Creating a policy	95

6.2.2. Viewing and editing policy settings	99
6.2.2.1. Viewing information about policy.....	99
6.2.2.2. On-demand scanning	100
6.2.2.3. Threats and Exclusions	103
6.2.2.4. Updating anti-virus databases and application modules.....	104
6.2.2.5. Working with system tasks	106
6.2.2.6. Setting up Quarantine and Backup storage.....	106
6.2.2.7. Producing report on the operation of application.....	108
6.2.2.8. Additional parameters.....	111
6.2.2.9. Viewing results of policy application.....	115
6.3. Managing tasks	116
6.3.1. Creating a task.....	116
6.3.1.1. Creating a local task	117
6.3.1.2. Creating a group task	123
6.3.1.3. Creating a global task	123
6.3.2. Viewing and editing task settings and monitoring task performance.....	124
6.3.3. Launching and stopping tasks.....	125
6.4. Configuring application settings	125
6.4.1. Viewing information about the application	126
6.4.2. Additional application settings	128
6.4.3. Working with the quarantine and backup storage areas.....	129
6.4.4. Viewing information on license keys	131
6.4.5. Setting up report generation parameters.....	131
CHAPTER 7. TESTING OPERATION OF KASPERSKY ANTI-VIRUS	132
7.1. Test “virus” EICAR and its modifications	132
7.2. Testing correct operation of Kaspersky Anti-Virus	133
CHAPTER 8. MANAGING LICENSE KEYS	136
8.1. Managing keys using local interface.....	137
8.2. Working with license keys using the Kaspersky Administration Kit interface..	140
CHAPTER 9. MANAGING APPLICATION FROM THE COMMAND LINE.....	141
9.1. Scanning selected objects	142
9.2. Full scan.....	144
9.3. Launching updates	145
9.4. Last update rollback	146

9.5. Starting the application	147
9.6. Stopping the application	147
9.7. Managing tasks	147
9.8. Import/export of settings	149
9.9. Adding a license key	149
CHAPTER 10. FREQUENTLY ASKED QUESTIONS.....	150
APPENDIX A. CONTACTING TECHNICAL SUPPORT SERVICE.....	156
APPENDIX B. GLOSSARY	159
APPENDIX C. KASPERSKY LAB.....	165
C.1. Other Kaspersky Lab Products	166
C.2. Contact Us	174
APPENDIX D. LICENSE AGREEMENT	175

CHAPTER 1. KASPERSKY ANTI-VIRUS SOS

Kaspersky Anti-Virus® SOS (hereinafter referred to as the Kaspersky Anti-Virus) is designed to protect workstations against computer viruses and malware.

The following features have been implemented in the application:

- **Protection against computer viruses and malware** – detection and elimination of malware in your computer. In the **on-demand computer scan**, the application will scan either the entire computer or individual disk, files or folders. You can launch this scan manually or configure this task to be launch automatically from time to time.
- **Recovering after a virus attack.** Full scan and disinfection that use settings recommended by the Kaspersky Lab's experts allows detecting all viruses that infected your data during virus attacks.
- **Updating of the anti-virus database and application modules** – updating of the anti-virus database with information about new viruses and attacks, methods to be used for disinfection of objects infected with these viruses and malware and updating of the application modules (if this feature is not disabled). Updates are downloaded from the Kaspersky Lab's updates servers, Kaspersky Administration Kit administration server or a server specified by the user or from a network/local updates folder.
- **Recommendations on the application setup and operation** – various tips and recommendation of Kaspersky Lab's experts on configuring the application to ensure the optimal anti-virus protection will be displayed when you use Kaspersky Anti-Virus.

Once dangerous objects are detected, if the anti-virus database has not been updated or the full computer scan has not been performed for a very long time, recommendations to perform certain actions with explanation will be displayed in the main window of Kaspersky Anti-Virus.

Based on the extensive practical experience in the anti-virus industry and on the analysis of the feedback provided by our users to the Technical Support Service, Kaspersky Lab's specialists did their best to configure the application to ensure the optimal performance.

- **The use of various application configuration profiles** – creating and using of special configuration files – *profiles* that store the application settings. By specifying application settings and saving them in the profiles you can easily alter Kaspersky Anti-Virus configuration. You can also

return to the recommended application settings at any time when using Kaspersky Anti-Virus.

- **Using two application operation modes** – you can use the application in the *user's* or the *administrator's* mode. In the user's mode only basic functionality of Kaspersky Anti-Virus is available, but you can not alter the application settings. In the administrator's mode you have access to all features to manage the application.
- **Placing objects into quarantine** – moving objects that are possibly infected with viruses and their modifications into a special safe storage where you can disinfect, delete them, restore them to the original folder or send them to the Kaspersky Lab's experts for analysis. Quarantined files are stored in a special format and do not impose any threat.
- **Creating backup copies of objects** – creating special backup copies of objects in a special storage before attempting to disinfect or delete these objects. Such copies are created for the cases when you need to restore the original object if it contains valuable information or to restore the situation when the infection took place. Copies are stored in a special format and do not impose any threat.
- **Creating reports** – registering all results of Kaspersky Anti-Virus operation in the reports. A detailed report about the results of the scan includes the general statistical information about objects scanned, stores information about the settings used to perform tasks and about the order of scan and processing of each particular object. Reports are also created for the results of the updates.
- **Centralized remote management of the application** – controlling the application using the Kaspersky Administration Kit 5.0 centralized administration system.



Some functions of Kaspersky Anti-Virus are available from the command line (details see Chapter 9 on page 141).

1.1. Hardware and software system requirements

In order to ensure normal operation of **Kaspersky Anti-Virus SOS**, your workstation must comply with the requirements listed below:

General requirements:

- 50 MB of free disk space;

- CD-ROM drive (for installation of Kaspersky Anti-Virus from a CD);
- Microsoft Internet Explorer 5.5 or above (in order to update the anti-virus database and the application modules from the internet).

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

- processor Intel Pentium 300 MHz or higher;
- 64 MB RAM.

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

- processor Intel Pentium 300 MHz or higher;
- 128 MB RAM.

1.2. Distribution kit

You can purchase the software from our distributors (retail box) or from one of our internet store (for example, www.kaspersky.com, **E-Store** section).

The retail box package includes:

- a sealed envelope with an installation CD containing the application files;;
- a user's manual;
- a license key included in the distribution package or recorded on a special floppy disk;
- registration card with the indication of the product's serial number;
- a license agreement.



Please read the license agreement carefully before opening the CD envelope .

If you purchase our product from an internet store, you will download it from the Kaspersky Lab site and the distribution package will also contain this guide. Your license key will be either included into the installation package or sent to you by e-mail upon the receipt of your payment.

1.2.1. License Agreement

The license agreement constitutes a legal agreement between you and Kaspersky Lab and contains terms and conditions subject to which you may use the purchased software.



Please read the license agreement carefully!

If you do not agree with the terms of the license agreement, you may return the box with Kaspersky Anti-Virus to the distributor, you have purchased it from; you will receive the full refund of the amount you have paid for subscription, provided that the envelope with the installation CD remained sealed.

By opening the sealed envelope with the installation CD or by installing the product to the computer you agree to all the terms and conditions of the license agreement.

1.3. Services for registered users

Kaspersky Lab offers its legal users a wide range of services that help to maximize the efficiency of Kaspersky Anti-Virus.

By purchasing a subscription, you become a registered software user, entitled to the following services throughout the period of subscription:





- software upgrades;
- consultation regarding issues pertaining to installation, setup and use of the software products available by phone or e-mail;
- notifications about availability of new Kaspersky Lab software products and about new viruses worldwide (this service is provided to users who have subscribed to the Kaspersky Lab e-mail newsletter).



No consultations are offered for issues pertaining to operating system functionality or to the use of various technologies.

1.4. Conventions

Various formatting features and icons are used throughout this document depending on the purpose and the meaning of the text. The table below lists the conventions used in the text.

Format feature	Purpose
Bold font	Titles of menus, menu items, windows, dialog boxes and their elements, etc.
 Note.	Additional information, notes
 Attention!	Information that requires attention
 <i>In order to perform action</i> 1. Step 1. 2. ...	Description of the successive user's steps and possible actions
 Task, example	Statement of a problem, example of the application's capabilities

CHAPTER 2. INSTALLATION AND REMOVAL OF THE APPLICATION

There are two options for installing **Kaspersky Anti-Virus 5.0 SOS**: local and remote installation (through the Kaspersky Administration Kit centralized administration system). This guide describes local installation of Kaspersky Anti-Virus to a workstation. For details regarding remote installation of the application, please consult the Kaspersky Administration Kit 5.0 Reference Guide.

2.1. Installing the application



We recommend that you close all applications running on your computer before you install Kaspersky Anti-Virus.

In order to install the application, run the executable file included in the distribution package



The process of installation from the installation package received via internet is completely analogous to the installation from the installation CD.

The installer works in the interactive mode. Each window contains a set of buttons for controlling the installation process. The purpose of these buttons is briefly explained below:

- **Next >** – confirm the action and switch to the next step of the installation process.
- **< Back** – return to the previous step of the installation process.
- **Cancel** – abort the installation process.
- **Finish** – complete the product installation process.

Following below is a detailed discussion of each step of the application installation.

Step 1. Verifying the version of the installed operating system

Before the application installation is started, a check will be performed to determine whether the operating systems and the Service Packs installed on your computer meet the software requirements for the installation of Kaspersky Anti-Virus.

If any of the requirements has not been satisfied, a corresponding notification will be displayed on the screen. We recommend that you install required software and service packs using the **Windows Update** service (or other appropriate services) before the installation of Kaspersky Anti-Virus.

Step 2. Starting window of the installer

Immediately after you have launched the executable file, the starting window will be displayed on the screen to inform you that Kaspersky Anti-Virus installation process has been started.

In order to proceed with the installation process, press **Next >**. In order to cancel the installation, press the **Cancel** button.

Step 3. Reading the License agreement

The **License Agreement** dialog box contains the text of the license agreement. Read it and then click **I Agree** if you agree with the terms and conditions of the agreement. In order to exit the installer press the **Cancel** button.

Step 4. Entering user's information

Enter the required user information in the **User Information** dialog box. Enter your name in the **User Name** field, and the organization in the **Company Name** field. By default the dialog box will contain information obtained from the Microsoft Windows register.

Step 5. Reading important information about the application

During this stage you will be offered to familiarize yourself with important information about the application. This window contains the major functions of Kaspersky Anti-Virus, peculiarities of its operation, etc.

In order to proceed to the next step of the installation process press **Next >**.

Step 6. Searching for other anti-virus software

During this step a search will be performed for any other anti-virus software installed on your computer, including Kaspersky Lab's software that can cause conflicts, if used jointly with Kaspersky Anti-Virus.

If other vendors' anti-virus software is detected installed on your computer, the installer will display a dialog box with a list of applications recommended to be removed before installing Kaspersky Anti-Virus.

We recommend that you uninstall such software. In order to do it, press the **No** button in order abort the installation process. Then uninstall the applications as required and run the executable file again.

If a copy of Kaspersky Anti-Virus 5.0 SOS has been detected installed on your computer, the version installed earlier will be updated by this application copy.



If you updated of version 5.0, the Install the license key dialog box (see Step 7 page 14) will not contain information about the key, but the key installed earlier will be used with the updated application.

Step 7. Installing the license key

You have to select the license key that will be used by Kaspersky Anti-Virus to verify your License agreement and determine its validity; the license key is selected using the **License Key** dialog box.



The license key is your personal "key" that contains all service information required for the full-featured functionality of the application, namely:

- support information (who is providing support and how you can get help);
- the license name, number and expiration date.



In order to install a new license key,

1. Press the **Browse** button and switch to the folder containing the license key:
 - If you purchased Kaspersky Anti-Virus in a box (retail box), your license key will be written on a floppy disk. You will have to enter the disk in the drive and select this drive to access the disk.
 - If you purchased your license online, save the license key file that you received by e-mail into any folder on the hard drive of your computer. Then switch to this folder.

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

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

After you do this, the installation wizard will display general information about the license and the path to the license key.

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

If, at the time of the installation, you still do not have the license key (for example you ordered it from Kaspersky Lab via internet but have not received it yet), you

can install this key later when you run the application or using a special license key installation utility (see Chapter 8 on page 136). Note that you cannot start using Kaspersky Anti-Virus without the license key.

Step 8. Selecting the installation folder

The folder into which Kaspersky Anti-Virus will be installed can be selected in the **Select installation folder** dialog box. When selecting the folder use the **Browse** button.

You can restore the path to the default installation folder using the **Restore** button; the default path is: <Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 5.0 SOS\.

The window that opens by the **Drive** button contains information about the available and required for the installation space on the logical drives of the workstation.


In order to proceed with the installation process, press the **Install** button. This will start the process of copying Kaspersky Anti-Virus files onto your computer.

Step 9. Completing the setup

The **Completing the setup** window displays information about completing of Kaspersky Anti-Virus installation on your computer.

Check the **Launch Kaspersky Anti-Virus** box if you would like to run the application immediately after the installation.

As the result of Kaspersky Anti-Virus installation:

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

2.2. Silent mode installation of the application

Kaspersky Anti-Virus 5.0 SOS can be installed from the command line. In order to install Kaspersky Anti-Virus, switch to the folder where the distribution file is located and use command:

```
setup [/s] [/l<report_file>] [/p<property>=<value>"..."]1
```

¹ Entries in square bracket are optional modifiers.

Modifier	Purpose
/s	Use the silent installation mode
/l<report_file>	<p>Output of events into the specified report_file.</p> <p>You can enter absolute or relative path to the file. If the path contains a space, it must be specified in double quotes.</p>
/p<property>	<p>Application installation settings.</p> <p>The following settings can be used:</p> <ul style="list-style-type: none"> • INSTALLDIR – full path to the application installation folder; • USERNAME – user name; • COMPANYNAME – user's company; • KLKEY – full path to the key file; • KLUNINSTPASSWD – password that will be asked for when you attempt to uninstall the application; • KLADMPASSWD – password for switching between the user's and the administrator's mode;

Example:

```
setup /s /l"C:/Kaspersky Lab/Report"
/pINSTALLDIR="C:/Kaspersky Lab" /pKLADMPASSWD=password
```

The silent mode installation settings can also be specified in the ini file in section [Setup].



The filename of the file containing the settings must always be **setup.ini**.

The following settings can be used:

- **InstallDir** – full path to the application installation folder;
- **User** – user name;
- **Company** – user's company;
- **Key** – full path to the license key file;

- **UninstallPassword** – password that will be asked for when you attempt to uninstall the application;
- **AdminPassword** – password for switching between the user's and the administrator's mode;

Example:

```
[Setup]
InstallDir=C:/Kaspersky Lab
Key=A:/License/00000001.key
User=Ivanov
```

2.3. Removing the application

If for some reason you need to uninstall Kaspersky Anti-Virus, run **Start → Programs → Kaspersky Anti-Virus 5.0 SOS → Kaspersky Anti-Virus Uninstall** or use standard Microsoft Windows **Add or Remove Programs** control panel tool.



If the application is controlled via Kaspersky Administration Kit, and password protection has been enabled to prevent its unauthorized uninstallation (see section 6.2.2.8 on page 111), you will be prompted for the password prior to the removal procedure.

You then will be prompted to confirm the removal. Click **OK** in order to start the removal process. This will open a window where you can choose whether quarantined and backup objects should be removed or preserved, as well as report and license key files.

That will start the process of removing the application files from the computer hard drive.



If during the process of removal the uninstaller detects files that can be used by other applications, you will see a dialog box that asks if you would like to delete this file. Click the **Yes** button in order to remove the file.

When removal of the application is completed, you'll be prompted to restart your workstation. Select the preferred variant and click the **Finish** button.

CHAPTER 3. APPLICATION MANAGEMENT CONCEPTS

Kaspersky Anti-Virus SOS is installed on a workstation and can be controlled locally or remotely through Kaspersky Administration Kit (if the computer is included into the centralized administration system).

There are several categories of users working with Kaspersky Anti-Virus:

- *Workstation user* is the computer user for the workstation on which Kaspersky Anti-Virus is installed.
- *Anti-virus security administrator* (hereinafter referred to as administrator) performs local management of Kaspersky Anti-Virus.
- *Logical network administrator* controls Kaspersky Anti-Virus operation via the centralized remote administration system Kaspersky Administration Kit.

Each user category is assigned its own interface providing access to all the software features which that category can use in accordance with their respective privileges.

The **user interface** is optimized for efficiency and simplicity and allows performance of the following tasks:

- review of status information pertaining to anti-virus protection;
- run file system objects scan tasks;
- update the anti-virus database and application modules (if such feature has been enabled by the administrator);
- review the results of tasks performance and the events log;
- review the content of Quarantine and Backup storage and send quarantined files to Kaspersky Lab for analysis.

In addition to the user's tasks, the extended **administrator's interface** allows to create file system objects scan tasks and updating tasks, to manage these task and to schedule when these tasks will be run.

If centralized administration via Kaspersky Administration Kit is used, the application is controlled remotely from a computer on which the *Administration console* installed.

The administration console is a standard **interface integrated into MMC** that allows the logical network administrator to perform the following functions:

- remote installation of Kaspersky Anti-Virus on client computers;
- updating the anti-virus database and application modules;
- managing policies and tasks on client computers;
- installing license keys to client computers;
- viewing reports about application operation on the client computers.



If you would like to control the application via Kaspersky Administration Kit, you will have to install the Network Agent on the client computer; the Network Agent ensures the interaction of the workstation with the Administration Server (details see Kaspersky Administration Kit 5.0 Reference Guide).

Please see details of the centralized administration concept in the Kaspersky Administration Kit 5.0 Administrator's Guide.

3.1. Basic concepts of the administration concept

When administrated locally, protection provided by Kaspersky Anti-Virus is configured by the administrator through modification of the application's settings and tasks.

A **task** is a specified action performed by the application. Based on their purpose, tasks are divided into types (full scan task, the task for updating anti-virus databases and software modules, etc.). Each task has a set of parameters (*task settings*) applied to its execution, i.e.

Application settings – a set of additional parameters defined for the operation of the application that includes parameters of the quarantine, backup storage, reports generation service, etc.

When using the centralized administration using Kaspersky Administration Kit, the administrator defines settings and tasks for the application installed on a remote computer of the network.

A distinctive feature of centralized administration is arranging of computers into groups and modifying their settings by creating and defining group policies.

A **Policy** is a set of application settings pertaining to its operation in a logical network group and a set of restrictions for redefining these parameters when configuring the application or a task.


A policy includes parameters required for complete configuration of the application's functionality, and includes both application settings and settings for



all types of tasks, except for parameters that must be defined each time a specific task is started.

3.2. Local interface

Kaspersky Anti-Virus has an intuitive and easy-to-use interface. This section contains a detailed description of its main elements: the system tray icon, right-click menu, main window, and some service windows.

3.2.1. System tray icon

After the application is launched, the application icon  appears in the system tray.

If a full computer scan or a scan of an individual file is in progress, a blinking icon  will appear in the system tray. During the download of the anti-virus database or of the application modules updates, the icon changes to .




If animation of the system tray icon is disabled in the additional settings of Kaspersky Anti-Virus (see section 5.8.4 on page 83), the icon will assume its original state.

If an important anti-virus event occurs, an informational message box appears for some time above the icon and displays a recommendation from the experts of Kaspersky Lab (in Microsoft Windows98/NT an additional window containing information about the event will open).

3.2.2. Right-click menu

If you right-click the application icon in the system tray, you will see a right-click menu (see Figure 1) consisting of the following items:

- **Open Kaspersky Anti-Virus** opens the **Protection** tab of the main application window. You can achieve the same result by a double left-click on the application icon  in the system tray.
- **Switch to user mode/Switch to administrator mode** – switch between the safety modes.
- **Running tasks** – a list of tasks launched according to the schedule. This item appears in the right-click menu when a certain task is being performed.

- **Scan My Computer for viruses** – launches a full anti-virus computer scan based on the defined level of protection.
- **Update Anti-Virus Database** – launches the anti-virus database update process.
- **About...** – displays a help window with information about Kaspersky Anti-Virus 5.0 SOS.
- **Exit** – close Kaspersky Anti-Virus. This item is accessible only by Kaspersky Anti-Virus administrator.



Figure 1. Shortcut menu

3.2.3. Main application window: general structure

The main window of Kaspersky Anti-Virus is designed for implementation of all application features, which helps achieve anti-virus protection of your computer. Here you can:

- start and stop full computer scan and scan of individual drives, folders and files for viruses and other types of malware;
- create user-defined objects scan tasks;
- download updates of anti-virus database and application modules.
- manage with quarantined objects;
- manage copies of objects created in the backup storage before they are disinfected or deleted;
- manage reports;
- control the application's configuration, etc.

All anti-virus protection settings, necessary information, and tasks are grouped in the following tabs of the main window:

- **Protection** – anti-virus protection status and tasks (scanning objects and updating the anti-virus database). From this tab you can access the functions that you can use to work with quarantine, backup storage and

reports. This tab is the main tab to be used for managing the application (see section 3.2.3.1 on page 22).

- **Settings** – the status and tasks for defining the main settings of the anti-virus scan (see section 3.2.3.2 on page 23).
- **Support** – a tab where you can view the information about the license key, renew the application license, access reference help and send your inquiries to the Technical Support Service (see section 3.2.3.3 on page 25).

Each tab is divided into two parts:

- *The left part of the tab* contains links that you can use to access tasks required when using Kaspersky Anti-Virus. The task list depends on the purpose of the tab. The **Protection** tab, for example, contains tasks for complete scanning for viruses, the **Settings** tab provides access to the anti-virus protection support tasks.
- *The right part of the tab* contains information about the **current** status of anti-virus protection (full system scan and the anti-virus database). Thus the **Protection** tab indicates the status of the anti-virus scan, the **Settings** tab shows the status of its settings and the **Support** tab displays the license status (license key information), links to support contact information, information about the application and your system.

3.2.3.1. The *Protection* tab

The **Protection** tab (see Figure 2) is designed for running tasks that ensure full system scan as well as scan of individual drives, folders or files. Here you can:

- launch the updating of the anti-virus database, application modules and network attacks database;
- switch to managing reports about the execution of all task you launch (view, delete, export to file);
- switch to managing quarantined objects that are possibly infected with viruses or their modifications;
- switch to managing backup copies of disinfected or deleted objects.

You can launch tasks using the corresponding links.



Figure 2. The **Protection** tab

The right part of the tab displays *the current state of the full computer scan and anti-virus database*. For example, on Figure 2 you can see that a full computer scan is currently in progress and that the anti-virus database is up-to-date. This tab also contains comments on the status of each anti-virus protection task.

Critical status and any status that is different from the recommended protection level are always supplemented with the *Kaspersky Lab's experts' recommendations*. In order to increase the level of the anti-virus protection you may be offered run a task, update the anti-virus database, etc. All recommendations are displayed as links that you can follow in order to perform the corresponding action.

If any infected or suspicious objects have been detected during the scan, the corresponding information will be displayed in the right part of the tab. Later you can switch to processing detected objects at any time by following the [process these objects](#) link (details see section 5.3 on page 59).

3.2.3.2. The *Settings* tab

The **Settings** tab (see Figure 3) contains information that you can use to evaluate the application's settings and to modify the settings of both main and additional settings of Kaspersky Anti-Virus.



Figure 3. The **Settings** tab

The right part of the tab displays the current settings of the on-demand full computer scan and automatic updating of the anti-virus database and application modules with detailed comments and tips on editing some settings. For example, if in the past you started the anti-virus database updating process manually, the application will suggest that you automate this process by creating a schedule to start this task automatically.

Following the links displayed in the left part of the tab you can switch to editing the on-demand scan and updating settings. You can also create a list of objects to be excluded from the scan scope and specify the type of the anti-virus database to be used.

Here you can also configure the setting of the quarantine that is used to store objects possibly infected with viruses or their modifications and of the backup storage used to store backup copies of objects. You can switch to configuring additional settings of Kaspersky Anti-Virus by following the [Additional settings](#) hyperlink.

Kaspersky Anti-Virus allows creating various configurations to be used in its operation and saving them in special files called *profiles*. Later you can easily return to the required configuration. In order to do this, you will not need to reconfigure the application as it will be sufficient to simply load the required

profile. You can switch to creating and loading profiles by following the [Managing profiles](#) link.

3.2.3.3. The *Support* tab

The **Support** tab (see Figure 4) displays contact information to be used when you need help if you encountered problems in the operation of Kaspersky Anti-Virus or a situation that you cannot handle by yourself. This tab also contains information about the application, the license key and about the operating system installed on your computer for cases when you need to provide this information to the Kaspersky Lab's Technical Support Service. This information is located in the right part of the tab.



Figure 4. The **Support** tab

The left part includes links that allow you to:

- send your inquiries and objects possibly infected with viruses and their modifications for analysis to the Kaspersky Lab's Technical Support Service.
- renew your Kaspersky Anti-Virus license.

The left part of the tab also contains links to the help information:

- [Help](#) – application reference system.
- [Virus Encyclopedia](#) – a link to www.viruslist.com site containing detailed descriptions of all currently existing malware.
- [Kaspersky Lab's Website](#) – a link to the Kaspersky Lab web site.

3.2.4. Scanning process window

The scanning process window appears on screen when a computer scan or scan of its individual objects (disks, folders, files) is launched (see Figure 5).

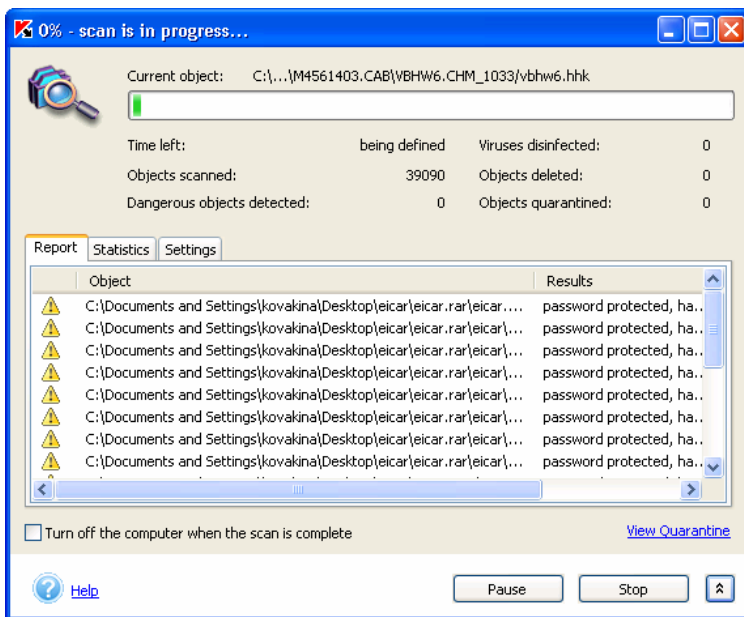




Figure 5. Scan process window

The window consists of two parts:

- The top part of the window contains an indicator showing the progress of the scan task in percents, the name of the object scanned, estimated remaining time and the general statistical data including the number of objects scanned by the moment and the number of objects that have been disinfected, deleted and quarantined.
- The bottom part of the window opens by pressing the  button and contains three tabs. **Report** – with the report about events that took place

during the scan, **Statistics** – with the scan results and **Settings** – with the list of settings used to perform the scan. In order to hide the bottom part, use the  button.

In order to access the quarantine window (see section 5.8.1.2 on page 74), follow the [View Quarantine](#) link.

If a full computer scan is being performed, you can use the same window to select a mode that turns off the computer after the scan is completed. This mode is useful if, for example, you start the computer scan at the end of the business day and you do not want to wait until it is finished.

However, the use of this mode requires the following preparation: before the scan is started, you have to disable prompting for password when scanning objects (see section 5.2.3.1 on page 51) if it is enabled, set automatic processing of dangerous objects, their deletion or placing into quarantine or recording information into the report (see section 5.2.3.2 on page 54). As the result of these actions, the interactive mode of the application operation will be disabled and the scan will not be interrupted (that is, prompts will not be displayed).

In order to turn off the computer after the scan is complete, check the **Turn off computer after the scan is complete** box in the scan window.

3.2.5. Help system


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

If you have a question on a particular dialog box, press the <F1> key or click [Help](#) in the bottom left-hand corner of the dialog box.

CHAPTER 4. COMPUTER PROTECTION USING THE DEFAULT SETTINGS

Immediately after Kaspersky Anti-Virus is installed, its default settings will be applied. These settings are recommended by the Kaspersky Lab's experts for ensuring the optimum protection of your computer.



If you are using centralized administration feature via Kaspersky Administration Kit, the settings can be determined by the policies and tasks created by the Security Administrator. This requires that a “lock”  is set on the corresponding settings. Details see Kaspersky Administration Kit 5.0 Reference Guide.

Additionally, there is a possibility for easy settings modification by selecting one of the three protection levels predefined by the Kaspersky Lab's experts: *maximum protection, recommended and maximum speed*.

4.1. Default settings

The default settings below are specified for each anti-virus protection task:

ON-DEMAND ANTI-VIRUS SCAN

The *recommended level* of protection with the following settings is the default level for full system scan:

- scheduled full scan is performed every Friday at 20:00;
- the scan scope includes:
 - all files on hard disks, and boot sectors;
 - files in RAM, objects launched automatically during operating system loading (startup objects), and alternate NTFS streams;
 - packed files, archives, self-extracting archives, and OLE objects.



Full computer scan does not include mailboxes

- iChecker™ technology is used;

- objects on network disks; e-mail databases, and files in e-mail text formats will not be scanned.
- If an infected or suspicious object is detected, Kaspersky Anti-Virus will postpone its processing until the anti-virus scan is completed, will prompt the user for action when the scan is finished and process the object.
- If a potentially dangerous software (riskware) is detected, Kaspersky Anti-Virus will skip it and save information about this program in the report;

UPDATING ANTI-VIRUS DATABASES AND APPLICATION MODULES

The default settings for updating anti-virus databases and application modules are:

- update procedure is scheduled to run every three hours from the moment of Kaspersky Anti-Virus installation;



If the computer works less than 3 hours a day, the database will be updated immediately after Kaspersky Anti-Virus is started next time.

- updating of anti-virus databases and critical Kaspersky Anti-Virus updates is enabled. A corresponding prompt will be displayed before the updates are installed.

ISOLATION OF SUSPICIOUS OBJECTS

The default settings for quarantine are:

- quarantine storage size is unlimited;
- objects are stored in the quarantine for 90 days.

SAVING A COPY OF AN INFECTED OBJECT

Prior to attempted disinfection or deletion, a copy of each infected object is saved in the backup storage. The default settings are:

- backup storage size is unlimited;
- backup objects are stored for 90 days.

4.2. Anti-Virus scan levels

In order to ensure easy modification of the anti-virus scan settings, the application provides for three levels with predefined settings (see Table 1).

- **Maximum protection** – the level of computer protection that corresponds to the maximum possible level of protection with some decrease in the system speed.

- **Recommended** – level of anti-virus protection based on the settings recommended by the Kaspersky Lab's settings that ensure optimal protection of your computer.
- **High speed** – level of computer protection that ensures maximum system performance with a certain decrease in the number of objects scanned.

If you modify the settings of any of the levels using the local interface or via the Kaspersky Administration Kit 5.0 Administration console, the value will change to the **User-defined settings**. This is the fourth level of the anti-virus protection with the user-defined settings.



If the settings have been changed via the Administration console, the right part of the **Protection** tab will indicate that the settings have been configured by the administrator.

The table below details the values of the settings of the predefined levels for for the on-demand scan.

Conventions:

- + enabled;
- disabled;
- x not provided for this task.

Table 1. Configuring scan level settings

Setting	Maximum protection	Recommended	High Speed
use IChecker	+	+	+
scan level	all files	all files	files of specified format
size of the object scanned, not more than, (MB)	–	–	8
scan time, not more than, (sec.)	–	–	60
hard drives	x	x	x
removable drives	x	x	x
network drives	x	x	x
NTFS streams	+	+	+
disk boot sectors	+	+	+
packed files	+	+	+
archives	+	+	–

Setting	Maximum protection	Recommended	High Speed
self-extracting archives	+	+	+
e-mail databases	+	-	-
mail text format files	+	-	-
OLE objects	+	+	+

CHAPTER 5. APPLICATION MANAGEMENT USING THE LOCAL INTERFACE

This chapter contains detailed information about operation and settings of the major tasks of Kaspersky Anti-Virus and additional features of the program control using the local interface.

5.1. Updating the anti-virus database and application modules

Kaspersky Anti-Virus provides a possibility to automate the updates of both the anti-virus database, which contains descriptions of viruses and methods to be used for their disinfection, and of the application modules, using the Kaspersky Lab update servers.



Updates of the anti-virus database are a prerequisite of anti-virus protection for your computer. Many new viruses appear daily and the Kaspersky Lab experts enter daily information about these viruses into the anti-virus database. We recommend that you update your anti-virus database each time before you start a scan task.




When downloading updates, Kaspersky Anti-Virus connects to Kaspersky Lab's http or ftp updates server specified by the user or to a local or a network folder on your computer. If you use Kaspersky Administration Kit to manage the application, the updates can be performed from the updates folder located on the *Administration server*.

You can launch the updater manually or schedule its start. In order to accomplish download of updated versions for the anti-virus databases on time, we recommend setting up a schedule for automatic launch of the updater (details on configuring the schedule see section 5.6 on page 68).

5.1.1. When to download updates

The application will inform you when the anti-virus database requires an update. You can also make your own judgment regarding the updates after reviewing their status in the right frame of the **Protection** tab (see Figure 2).

The status of updates is indicated by the following icons:

-  *anti-virus database has been updated recently* or is being currently updated
-  *anti-virus database update required*. If updating is not possible because the license key has expired, the application will offer to read information about the license renewal
-  *urgent update required* as the anti-virus database is totally outdated, missing or corrupted.

5.1.2. Performing manual update.

Downloading updates



In order to launch the update process manually,

use the [Downloading updates](#) hyperlink in the left frame of the **Protection** tab.

or:

the [update the anti-virus database](#) hyperlink from the notification about the status of the anti-virus database in the right frame of the **Protection** tab;

or:

select the **Update Anti-Virus Database** item in the pop-up menu, which appears when you right-click the application icon in the system tray.

This will open a window (see Figure 6) containing information about the progress of the anti-virus databases and application modules updating.

The update downloading procedure can be divided into the following steps:

1. Kaspersky Anti-Virus checks connection to the network and establishes connection with the source of updates.
2. The application obtains a list of updates and information on their size from the Kaspersky Lab update servers.
3. The program compares the status of the anti-virus database and the application modules on your computer with those located at the update source. If your computer has the latest version of the anti-virus

databases the updating process will be complete. Otherwise files will start being copied to your computer.

The downloading progress is displayed using the copying process indicator. The size of the received updates is indicated in the **Updates downloaded** field.

4. The program automatically connects downloaded anti-virus database. If the database is connected successfully, Kaspersky Anti-Virus will start using the database to scan the computer. If the new anti-virus database connection results in an error, the database will be automatically rolled back to the previous version.



In order to ensure correct connection of the received updates you may need to reboot your computer. In this case, a corresponding warning will be displayed.

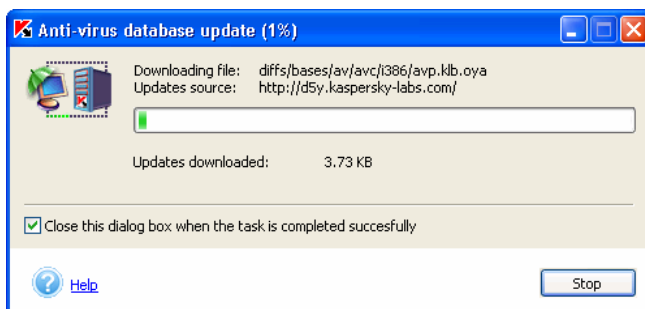


Figure 6. Updating the anti-virus database and application modules

5.1.3. Configuring updates



In order to configure the settings of the anti-virus database update task:

use the [Configure Updater](#) hyperlink in the left frame of the **Settings** tab (see Figure 3).

This will open the **Updating the anti-virus database** window (see Figure 7).

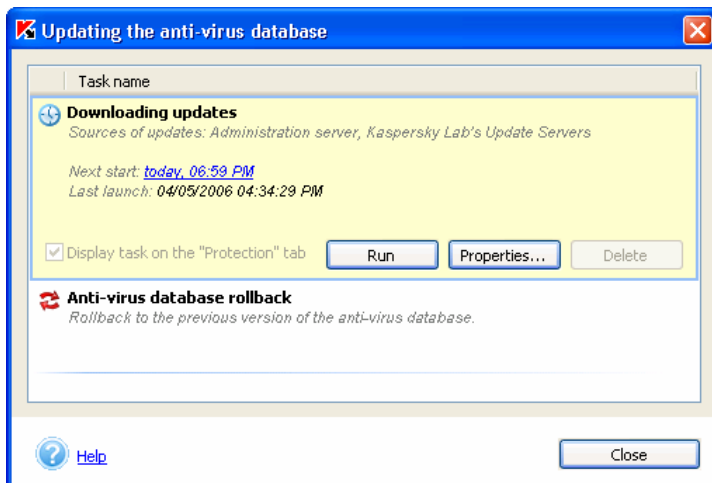


Figure 7. List of anti-virus database update tasks

Block containing information about the update source and about the start time of the last and the next update procedure is opened by a mouse click on the task name. Using this block you can launch the anti-virus database updating manually using the **Run** button or using the **Properties...** button - open the anti-virus database update settings configuration window (see Figure 8) where you can:

- create a schedule for automatic launch of the updating process (see section 5.6 on page 68);

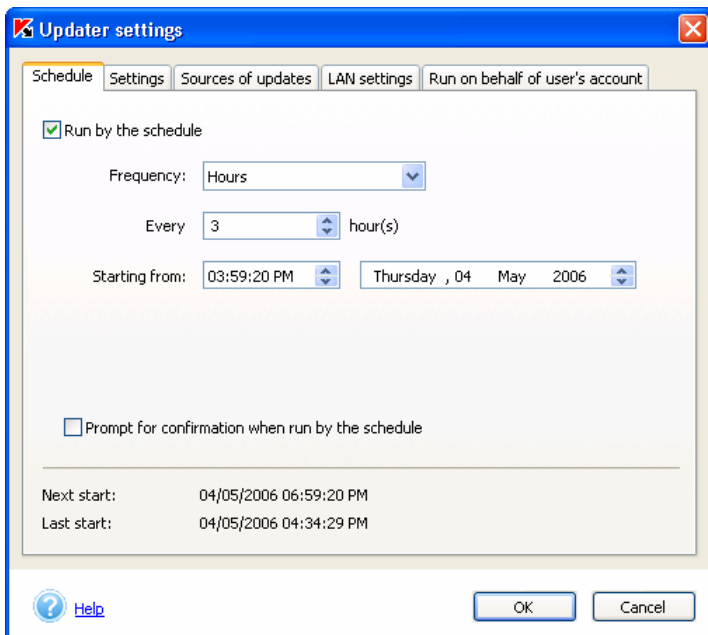


Figure 8. Anti-virus database updating task settings configuration

- enable Kaspersky Anti-Virus application module updating feature (see section 5.1.3.1 on page 37);
- configure the feature of copying updates into a local folder for broadcasting to other network computers on which Kaspersky Anti-Virus is installed (see section 5.1.3.2 on page 38);
- select the updates source; Kaspersky Lab's http or ftp updates server, indicated by the user or a local or network folder (see section 5.1.3.3 on page 39);
- configure the proxy server settings (see section 5.1.3.4 on page 41);
- configure the start of the task under a different user's account (only for computers running Microsoft Windows NT/2K/XP) (see section 5.7 on page 71);
- select the type of the anti-virus database to be downloaded (see section 5.1.3.5 on page 42).



The **Anti-virus database rollback** does not include any settings. You can only launch this task in order to return to the previous version of the anti-virus database.

5.1.3.1. Updating the application modules

Apart from the anti-virus database you can also update the Kaspersky Anti-Virus application modules. Application modules updates files are uploaded to the updates servers as they are released.

You can update the application modules from the updates source specified during the application setup (see section 5.1.3.3 on page 39). In order to do this it is sufficient to check the **Install application modules updates** box on the **Settings** tab of the **Updater settings** window (see Figure 9). Select which updates you would like to install:

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

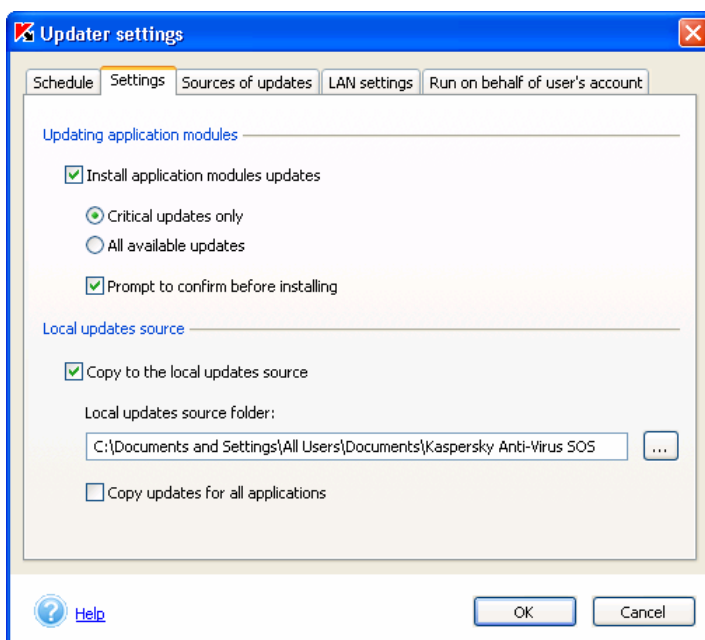


Figure 9. Updating settings configuration window.
The **Settings** tab

If you want the application modules updates to be installed automatically once they are downloaded, uncheck the **Prompt to confirm before installing** box.



If you order a zip archive with the updates from the Kaspersky Lab or from one of its partners, please make sure to indicate that you would also like to receive the application modules updates.

When you receive the application modules a corresponding prompt will be displayed on the screen (see Figure 10). Select one of the following options:

- **Install application modules updates.**
- **Do not install application modules update, remind later** – remind about installation of the application modules update next time Kaspersky Anti-Virus is launched.
- **Disable application modules updates installation** - if you select this option, the **Install application modules updates** box on the **Settings** tab of the **Updater settings** (see Figure 9) will be unchecked and the application modules updates feature will be disabled.

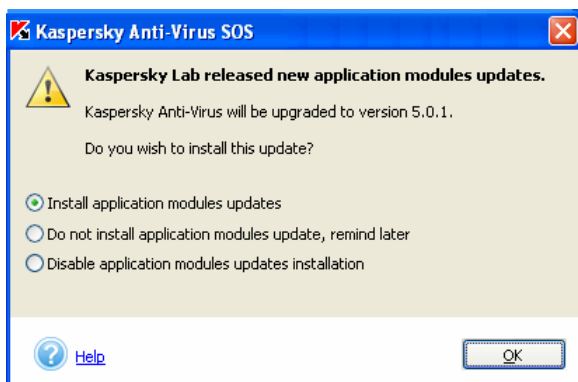


Figure 10. Prompt for installation of the application modules

5.1.3.2. Copying updates to the local folder

You can configure the operation of the updates copying service on the **Settings** tab (see Figure 9). This service allows to save the anti-virus database and the application modules updates received from the Kaspersky Lab's update service into a local folder and to allow access to this folder for other computers in the network (on which Kaspersky Anti-Virus is installed) in order to save internet traffic.

In order enable the updates copying service, check the **Copy to the local updates source** box. Specify the path to the folder in the **Local updates source folder** text field.

In addition, you can select the updates copying method:

- *full* to copy the updates of the anti-virus database and of the modules for all Kaspersky Lab's applications. In order to select full update, check the **Copy updates for all applications** box.
- *selective*, which will include copying of the anti-virus database and application modules updates only for Kaspersky Anti-Virus 5.0 SOS and Kaspersky Anti-Virus for Windows File Servers. In order to select this method of updating, the **Copy updates for all applications** box must be unchecked (it is checked by default)

5.1.3.3. Selecting the updates source

You can select the updates source on the **Sources of updates** tab of the **Updater settings** window (see Figure 11).

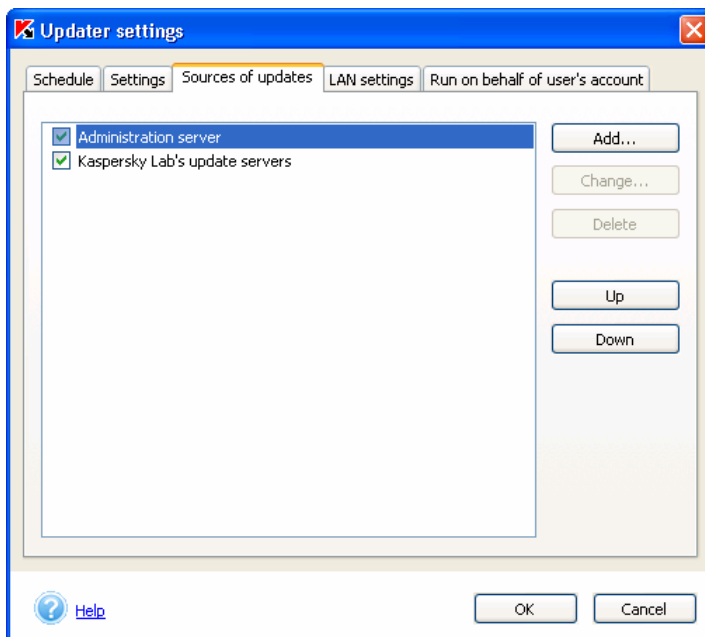


Figure 11. Updates settings window.
The **Sources of updates** window.

You can specify the following as the updates source:

- *Administration server* – a centralized updates storage located at the Kaspersky Administration Kit Administration Server. This updates source will not be available if the Network Agent is not installed on the computer (details see the Kaspersky Administration Kit 5.0 Reference Guide).
- *Kaspersky Lab's update servers* – Kaspersky Lab's internet sites on which updated anti-virus database and application modules are uploaded.
- *ftp-, http-servers*, added by the user and containing the new updates.
- *a local or a network folder*

By default, the updates are downloaded from the Kaspersky Lab's internet updates services or from the Administration Server if you use Kaspersky Administration Kit 5.0. You can expand this list with additional updates sources. In order to do it, press the **Add** button and select the type of source - *an Updates server's address or a Folder*. If you selected the *Updates server's address*, enter the address of the ftp- or an http- server in the window that will open (when you specify the server name you will have to enter the prefix of the protocol you are intended to use, for example, *http://server.net* or *ftp://10.0.0.1*). If you selected *Folder*, specify the path to the folder that contains the updates.

You can modify the updates source settings using the **Change** button. You can change the address for the *Updates source* type source or change path for the *Folder* type source.

You can select the region for the Kaspersky Lab's server from which the updates will be copied by selecting the corresponding country from the **Location** drop-down list (see Figure 12). By default the country will be selected based on your operating system's regional settings. We recommend that you specify your current location in order to determine the server closest to you. This will increase the speed and shorten the time required to download the updates. You can also disable the use of the proxy server by checking the corresponding box.

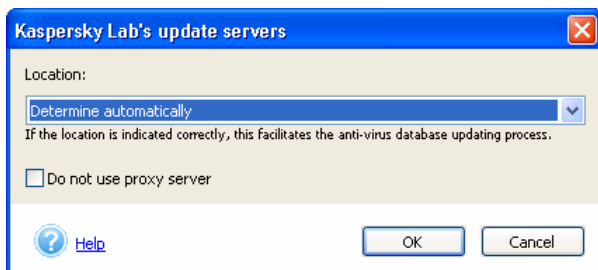


Figure 12. Changing the settings of the updates source. Selecting the geographical region of the server's location.

If you wish the updates to be performed from the specified source, check the box next to it. You can select several resources at the same time. In this case Kaspersky Anti-Virus will perform updates from the first source in the list. If this source is unavailable for any reason, the updating will be performed from the source next in the list, etc. You can change the order of the sources in the list using the **Up** and **Down** buttons.

If you do not have access to the Kaspersky Lab's updates servers (for example, if you do not have internet access), you can call our central office (+7 (495) 797-87-00 and inquire about locations of Kaspersky Lab's partners who can provide you with the anti-virus database on floppy or compact disks in zip format.



When your order your anti-virus database, specify which type of database (standard or extended) you would like to receive (see section 5.1.3.5 on page 42).

Unpack the zip archive with the anti-virus database in any folder on your computer and set this folder as the updates source.

5.1.3.4. Proxy server settings configuration

The network connections settings can be configured in the **LAN Settings** window (see Figure 13). There are two methods to determine the proxy server settings:

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

The first option is the default option, in this case the settings will be copied from Microsoft Internet Explorer. If the proxy server requires authorization, select the second option and specify the proxy server settings manually:

Address – IP address of the proxy server in the decimal format, for example 10.10.10.102 or its name.

Port – number of the port where the proxy server is installed. Select one of the suggested values: 3128, 8080, 8082, 8903 from the drop-down list or enter your own value.

If the proxy server requires authorization, check the **Use proxy server authorization** box and enter the username and the password as required in the fields below.

If proxy server authorization is required and you have not entered the username and the password or if the values you entered have not been accepted by the proxy server, a window with a prompt for the username and the password for authorization purpose will open when you start the updating process. If the authorization is successful, the specified username and the password will be

used for the next update. Otherwise you will be prompted for the authorization parameters again.

If your server has a firewall and you cannot connect to the required FTP server in the active mode check the **Use passive mode when updating from FTP servers** box.

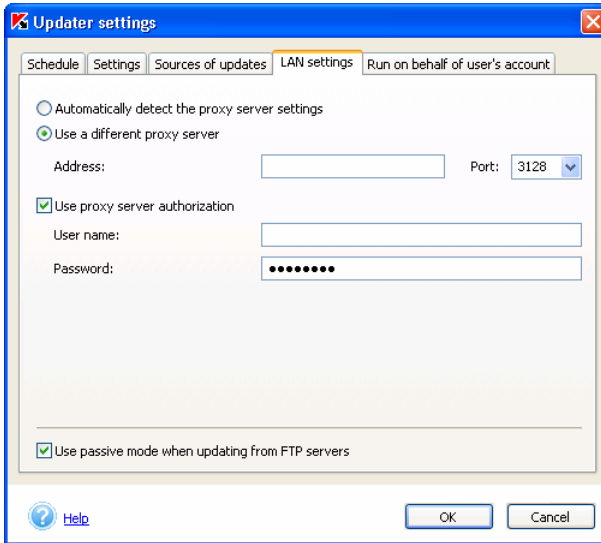


Figure 13. Configuring LAN settings

5.1.3.5. Selecting anti-virus database type

Kaspersky Anti-Virus offers the choice of two anti-virus database types that can be used by the application:

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



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



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

1. Follow the [Threats and exclusions](#) link in the left section of the **Settings** tab (see Figure 3).
2. If you wish to use the extended anti-virus database, check the **Adware, riskware, automatic dialers** box in the **Detectable threats** section of the dialog box that will open. In order to avoid deletion of programs that you use we recommend that you select an action requiring user's conformation as the action to be performed upon detection of a dangerous object.



The **Viruses, worms, trojans, hacking utilities, spyware** box is checked by default and cannot be unchecked. This indicates that standard anti-virus database is used for the scan.

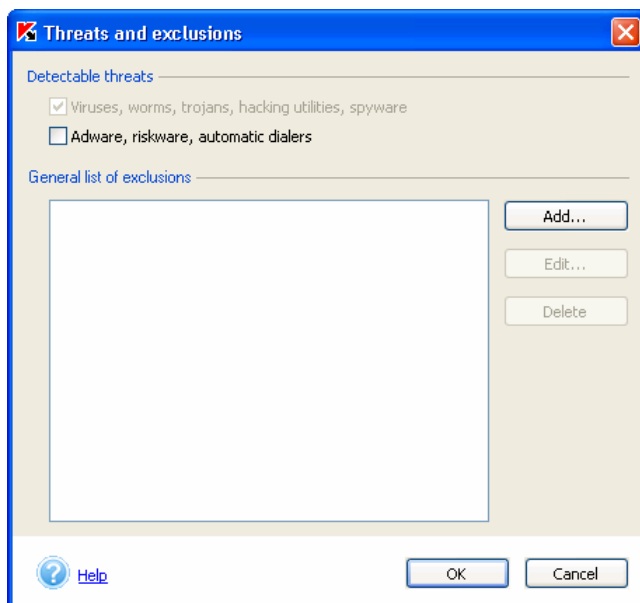


Figure 14. Selecting anti-virus database type

5.2. The on-demand scan mode

On-demand scanning is the mode of the application designed to scan for the presence of malicious code at the request of the workstation user or

administrator, and disinfect and remove infected objects as well as quarantine suspicious objects.

Kaspersky Anti-Virus allows scanning of the entire computer or of its parts - individual disks, folder, files, mail. The scan involves disinfection and deletion of detected dangerous objects and placing suspicious objects into quarantine.

The following system on-demand scan tasks will be created by default during the installation of the application:

- **Scan My Computer** – full scan of the entire file system of the user's computer (see section 5.2.1 on page 44) will be launched automatically every Friday at 8:00 pm.
- **Scan removable drives** – scan of removable media (floppy disk, CD, flash card, etc.), by default is launched manually by the user (see section 5.2.5 on page 58).
- **Scan critical areas** – scan of the system memory, startup objects, disk boot sectors, *Windows* and *Windows/System32* system folders is by default launched manually by the user.
- **Scan Quarantine** – scan of the quarantine objects is by default launched manually by the user.
- **Scan at Kaspersky Anti-Virus startup** – scan of the startup objects, system memory and disk boot sectors, by default this scan is launched automatically at Kaspersky Anti-Virus startup.

You can also scan an individual object that you specify (details see section 5.2.2 on page 46). Besides, you can create additional on-demand objects scan tasks (see section 5.4 on page 63).






For successful disinfection of Microsoft Outlook Express mail databases, you must close Microsoft Outlook Express before scanning.

5.2.1. Full computer scan

Full scan allows scanning larger number of objects than with the real-time protection, therefore for preventive purposes we recommend that you perform full computer scan at least once a week.

The application will prompt you when you need to perform full scan. If the main application window is closed, then a message will appear above the Kaspersky Anti-Virus icon in the system tray with a recommendation to start scan (if pop-up messages are not disabled, see section 5.8.4 on page 83).

In order to read more details, open the main application window on the **Protection** tab (see Figure 2) and note the full scan status in the right section of the window. The full scan status can be one of the following:

-  *scan is performed on a regular basis or is being performed at the moment;*
-  *it is necessary to launch scan, possibly you will need to return to the settings recommended by the Kaspersky Lab's experts;*
-  *you must perform a full computer scan immediately.*

If required, you can launch the scan immediately from the full scan status section by following the [perform a full computer scan](#) link.

Kaspersky Lab's experts recommend that users enable scheduled full scan mode. The full scan status includes information on whether this mode is enabled.

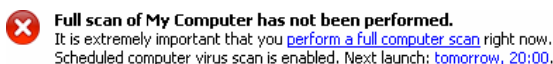



Figure 15. Scan status information




*In order to launch an on-demand anti-virus scan select the following in the left part of the **Protection** tab:*

[Scan My Computer](#) launches a full system scan in accordance with current settings (see below). The same result can be achieved using the [perform a full computer scan](#) hyperlink in the right frame of the **Protection** tab and the **Scan My Computer for viruses** menu item of the menu displayed when the user right-clicks the  icon in the system tray.

After this the **Scan** window will open (see Figure 5) that displays the task execution progress in percents, the name of the object currently being scanned, the estimate scan completion time and the general statistics information that contains the number of objects scanned by this moment as well as disinfected, deleted and quarantined objects.



The full computer scan does not include analysis of mail boxes, removable drives and network drives if such drives are connected to your computer.

You can hide the scan window by pressing button  in the right top corner and select **Close this dialog box and resume scan** in the window that will open.

You can view the scan results in the report (details see section 5.8.2 on page 78).

5.2.2. Scanning selected objects

You can select an object to be scanned using either Kaspersky Anti-Virus interface or standard Microsoft Windows tool (for example, using your **desktop** or **Windows Explorer**, etc.)



In order to select an object to be scanned using Kaspersky Anti-Virus interface,

follow the [Scan objects](#) link in the left section of the **Protection** tab (see Figure 2).

The **Select objects to scan** window (see Figure 16) contains the list of objects that can be scanned and the list edit and scan control buttons.

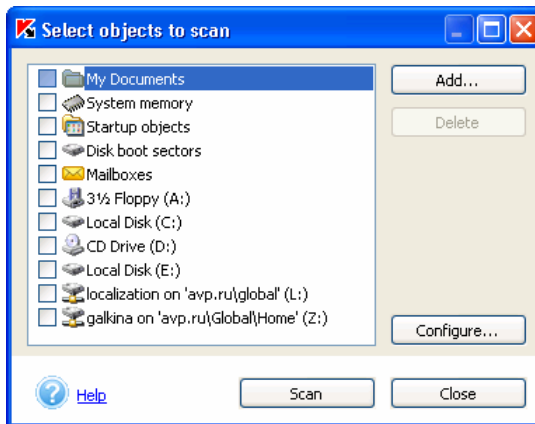


Figure 16. Selecting objects to be scanned

The original list already includes some objects.

- removable drives (including floppy disks and CDs);
- hard drives;
- network drives (if such drives are connected to your computer);
- Microsoft Office Outlook and Microsoft Outlook Express mailboxes;
- **My Documents** folder;

- system memory;
- startup objects;
- disk boot sectors.

If you would like to add a new object to the list, press the **Add** button and specify the required file or folder in the window that will open. All objects added by you in the list will be saved for subsequent scans.



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

In order to remove an object from the list, select it and press the **Delete** button. However you have to remember that you can remove from the list only those objects that were added manually. Object that had been included in the list originally, cannot be removed.

If you would like to change the settings used to scan selected objects, use the **Configure** button (details see section 5.2.3 on page 48). Settings entered will be saved for scanning of objects included into the list in the future and for scanning objects selected using standard Microsoft Windows tools.



In order to scan some of the objects from the list,

1. Select objects from the list.
2. Press the **Scan** button to launch the scan.



In order to launch object scan selected using standard Microsoft Windows tools,

Select the object with the mouse, right-click to open the Microsoft Windows shortcut menu and select the **Scan for viruses** item (see Figure 17). Settings specified in the **Select objects to scan** window will be used for scanning (see Figure 16).

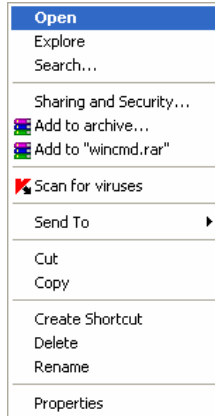


Figure 17. Scanning objects selected using Microsoft Windows tools



If Kaspersky Anti-Virus is not running, then you will be offered to launch it when you initiate the scan of the object selected using Microsoft Windows tools.

Irrespective of the method used to start the object scan (from the Microsoft Windows shortcut menu or from the Kaspersky Anti-Virus list of objects) a **Scan** window will be displayed (see Figure 5). You can view the scan results in the report (details see section 5.8.2 on page 78).

If you scan some objects on a regular basis, you can create a corresponding on-demand task (details see section 5.4 on page 63).

5.2.3. Configuring on-demand scan



In order to view or modify the on-demand scan settings,

follow the [On-Demand Scan tasks](#) link in the left section of the **Settings** tab (see Figure 3).

This will open the **On-Demand Scan tasks** window (see Figure 18) containing the list of system tasks and the list of additional scan tasks created by the user.

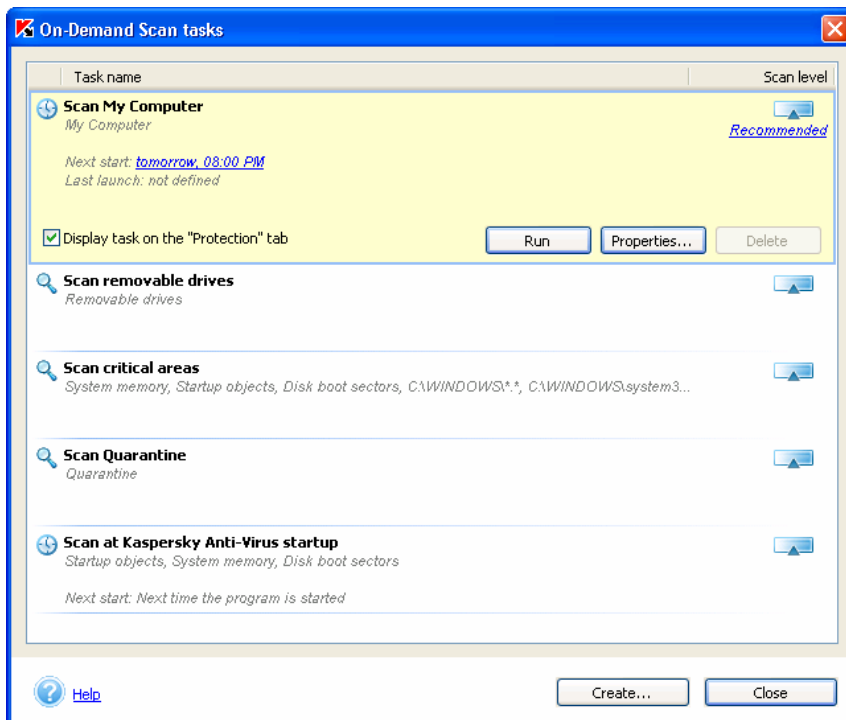


Figure 18. On-demand scan tasks list

Block containing information about the scan scope and about the start time of the last and the next scan is opened by a mouse click on the task name. Using this block you can launch an on-demand scan using the **Run** button or open the anti-virus scan settings configuration window (see Figure 19) where you can:

- select objects to be scanned. only tasks created manually can be selected. In order to add a new object, press the **Add** button and select the object you need from a drop-down list. In order to scan an object not included into the list, for example, an individual folder or a file, select the **Browse** line in the list and specify path to this object. In order to delete an object from the list of objects to be scanned, select it in the list and press the **Delete** button;

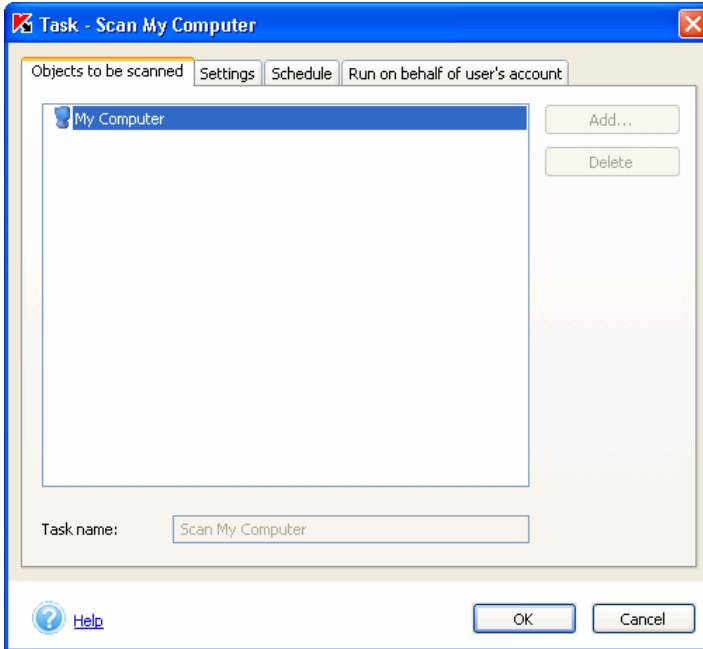



Figure 19. On-demand scan task settings window. The **Objects to be scanned** tab


- specify the anti-virus protection level, perform a detailed configuration of the selected level (see section 5.2.3.1 on page 51);
- create a list of objects that will not be scanned (see section 5.5 on page 64). In order to access the window to be used to create the exclusions lists, press the [not specified/specified](#) link next in the description of the selected protection settings. The appearance of the link changes depending on whether any exclusion are specified;
- select action that will be used by Kaspersky Anti-Virus upon a detection of dangerous and suspicious objects (see section 5.2.3.2 on page 54).
- set up a schedule for automatic scan tasks launch (see section 5.5 on page 64);
- configure the start of the task under a different user's account (only for computers running Microsoft Windows NT/2K/XP) (see section 5.7 on page 71);

If you plan to launch a task frequently, we recommend that you check the **Display task on the "Protection" tab** box in the information section of the task.

In this case you will be able to launch such task by clicking on the link with its name, located in the left section of the **Protection** tab (see Figure 2).

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

 – this icon indicates that for a schedule has been setup for this task to be used to ensure its automatic launch.

 – indicates that the task is currently running.

In order to create an additional scan task, use the **Create** button in the **On-Demand Scan tasks** window (see Figure 18). Details about creating the task see section 5.4 on page 63.

In order to remove the task, select it in the list and press the **Delete** button. However you have to remember that you can remove from the list only those tasks that were added manually. System tasks cannot be deleted. Besides, you cannot delete tasks that are being performed at the moment.

5.2.3.1. Selecting the scan level

Select one of the levels pre-defined by the Kaspersky Lab's experts (see Figure 20) in the **Scan level settings** drop-down list on the **Settings** tab (see section Chapter 4 on page 28). By default the recommended anti-virus scan level settings will apply.

You can configure your own settings based on the settings of any level. In this case the protection level will be changed to **User-defined settings**. Such user-defined settings will not be saved when you return to the settings of any of the three pre-defined levels.

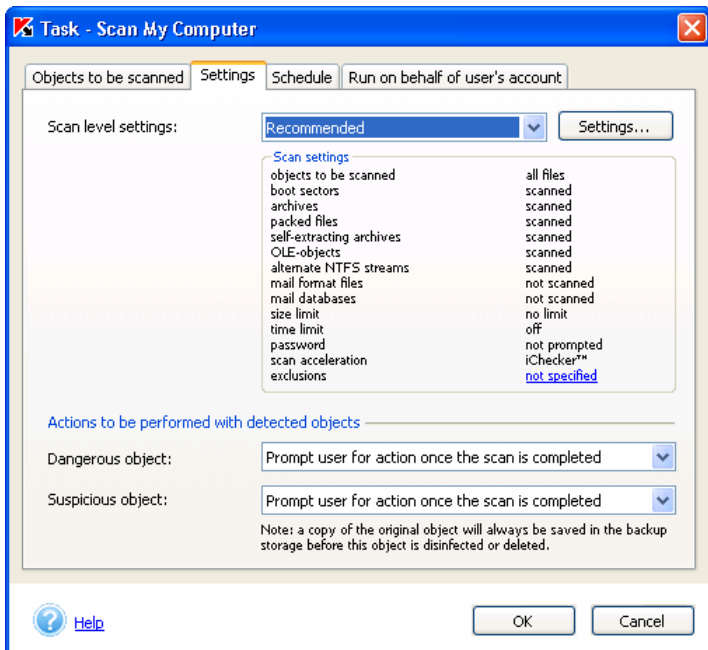


Figure 20. Configuring an on-demand scan

You can view and modify settings of the selected level in the **On-demand scan settings** (see Figure 21) that opens by pressing the **Settings** button (see Figure 20).

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

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

Using the **Additional scan settings** section you can determine whether the following objects will be scanned:

- boot sectors;
- archives;

- packed executable files;
- self-extracting archives;
- objects attached or built-in into other files (*OLE-objects*),
- alternate NTFS streams;
- mail files;
- mail databases

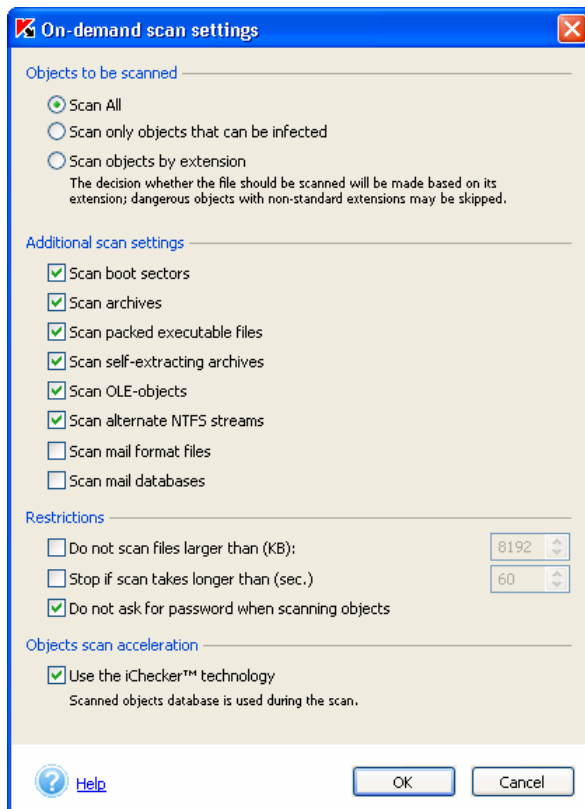


Figure 21. Fine-tuning an on-demand scan

Check the following boxes in the **Restrictions** section:

- **Do not scan files larger than (KB)**, to restrict the size of the objects being scanned specify the maximum size of the object (in KB) to be scanned.
- **Stop if scan takes longer than (sec.)** in order to restrict the scan time for one object specify the scan interval in seconds.
- **Do not ask for password when scanning objects** in order to prevent displaying the prompt for password while objects are being scanned. If this box is checked, password-protected objects will be skipped during the scan.

In the **Objects scan acceleration** you can enable/disable the use of the anti-virus scan acceleration technology iChecker™. In order to do it, check the corresponding box.

5.2.3.2. Actions to be performed with a detected object

In the **Actions to be performed with detected objects** section (see Figure 20) select the action type to be performed when such object is detected:

- **Prompt user for action once the scan is completed** – suggest to process dangerous object after the scan is completed. This mode is selected by default as it does not require your presence while the scan is being performed. Since the scan may take a long time, we recommend that you use this mode when you cannot control processing of dangerous objects as soon as they are detected.
- **Prompt user for action during the scan** – display prompts for actions to be performed with objects during the scan. The prompt will list all possible actions that can be performed with the object and one of such actions will be marked as recommended by the Kaspersky Lab's experts. This mode of the program's operation should be selected if you do not plan to leave your computer during the scan.
- **Perform the recommended action** – perform action recommended by Kaspersky Lab's experts. Recommended action is always well-justified, therefore you can select this mode in most of cases. The following actions are recommended:

- *Disinfect infected object, delete if disinfection fails*².
- *Quarantine the object* possibly infected with a virus or its modification.



Sometimes as the result of placing the file into quarantine, a message can be displayed informing the user that this object cannot be deleted. This is related to the fact that placing an object into quarantine involves moving this object: copying it to the quarantine and deleting it from its original location. However, some objects cannot be deleted when they are moved, for example, an object currently in use by another application.

- *Delete* a dangerous object if it is a trojan horse or a worm.



If an infected / potentially infected object is a riskware, then such object will be *skipped*.

- **Disinfect, delete if disinfection fails** – attempt to disinfect a dangerous object, delete if disinfection is not possible. In this case, potentially dangerous objects will also be disinfected and deleted if they cannot be disinfected. Before the object is attempted to be disinfected a backup copy will be saved in the backup storage.
- **Delete objects** – delete dangerous object detected during the scan without attempting to disinfect it and without prompting use for confirmation. When an object is deleted, its copy will be saved to the backup storage. We recommend that you select this mode of Kaspersky Anti-Virus operation only if you are sure that you will not lose valuable information.
- **Report only** - do not perform any action with the object, record information about infection into the application's operation report. We recommend that you select this mode operation in very rare cases as in this case dangerous and malicious objects will remain in your computer.

There are situations when it is impossible to perform action with the object. For example, when an infected object is in use by another application at the moment it is to be scanned, such object can not be processed. In this case a corresponding message will be displayed (see Figure 22), where you will be offered to perform one of the below actions:

- *Disinfect at system startup*. This action will be listed only if this object can be disinfected.

² By default infected RAM objects will be deleted and boot sectors infected with viruses will be disinfected and blocked if disinfection is not possible.

- *Delete at system startup.*
- *Skip* - do not perform any action with the object, record information about its detection into the application's operation report.


If you close the prompt window using the  button in the top right corner, the action selected in this window will not be performed and the object will be skipped.



Figure 22. Immediate disinfection of the object is impossible

5.2.4. Scanning archives

Kaspersky Anti-Virus scans archives if the archives scan was not disabled (that is if the **Scan archives** box in the **On-demand scan settings** window has not been unchecked), see Figure 21.



**Kaspersky Anti-Virus scans all objects within archive, but disinfects only objects in zip, arj, cab, rar, lha and ice archives.
Kaspersky Anti-Virus DOES NOT DISINFECT self-extracting archives!**

If an archive or an object within an archive is password-protected and the password prompt mode is enabled, then a prompt for a password will be displayed before such archive or object is scanned (see Figure 23). If you selected the delayed object processing mode (that is if the **Prompt user for action once the scan is completed** action is selected in the settings, see section 5.2.3.2 on page 54), a prompt for the password will be displayed after the scan is completed.



You can choose whether the prompt for the password is displayed by checking or unchecking the **Do not ask for password when scanning objects** box in the scan settings (see section 5.2.3.1 on page 51). By default, only the checkbox for the **Maximum protection** level is unchecked.



Figure 23. Entering password to scan an archive

In the **Password** field, enter the password to be used to access the archive file and click **OK**. The application will continue scanning the archive and the objects it contains after the password is entered.



While processing (disinfecting, deleting) objects within archives, Kaspersky Anti-Virus unpacks the archive being processed into a temporary folder, scans its objects, processing objects, packs them back using the same name and copies to the original location, replacing the original existing archive. The same processing procedure is provided for processing password-protected objects contained in the archive. The difference is that after the processing objects will be packed into the archive without using the password.

To scan another password-protected archive, Kaspersky Anti-Virus automatically applies the password used for the previous archive to the next archive to be scanned. If the password is incorrect, you will be asked to enter a new password.

If you do not know the password, the application will be unable to scan password-protected archives. We recommend that you click **Skip** and proceed with the scan.

If an archive file contains password-protected objects, click the **Skip archive** button to exclude them from the current scan. All other objects inside the archive that are not password-protected will be scanned and processed in accordance with the settings defined for anti-virus scanning.

The **Apply to all password-protected objects within this session** box applies to the action selected after it is checked.

For example, if you checked this box and then select **Skip**, **Skip archive**, then the remaining password-protected objects will not be scanned. Or, if you enter the password and click OK, then the application will attempt to apply that password to all the remaining password-protected objects without displaying a dialog box.

If the archive cannot be disinfected and if you selected **Perform the recommended action** as the action to be performed upon a detection of a dangerous object, Kaspersky Anti-Virus will not delete the archive and will only enter information about its detection in the report.

If you selected **Prompt user for action once the scan is completed** or **Prompt user for action during the scan** (see section 5.2.3.2 on page 54) as the action to be performed in the scan settings, you can delete the archive that can not be disinfected by selecting the **Delete** action in the dialog box with the prompt. Alternatively, you can delete this archive manually.

5.2.5. Scanning removable drives

You can start a removable drives scan from the main Kaspersky Anti-Virus window or from the Microsoft Windows shortcut menu that you can open, for example, in the **Windows Explorer** or **Desktop** window, etc.



In order to scan removable drives from the Microsoft Windows shortcut menu,

select drives (you can select CD drive and floppy drive at the same time), right-click to open Microsoft Windows shortcut menu and select **Scan for viruses** from the menu (see Figure 17).



In order to scan a CD or a floppy disk for viruses from the main application window of Kaspersky Anti-Virus,

1. Insert the CD or the floppy disk into the corresponding drive. Please pay attention that the program can scan both the CD and the floppy disk at the same time.
2. Follow the [Scan removable drives](#) link in the left section of the **Protection** tab (see Figure 2). This link is displayed if the **Display task on the "Protection" tab** box in the information section of the task is checked (see Figure 18).

or

Follow the [Scan objects](#) link to switch to the **Select objects to scan** window (see Figure 16), select removable drives and press the **Scan** button.

or

Select the **Settings** tab in the main application window and follow the [On-Demand Scan tasks](#) link. This will open the **On-Demand Scan tasks** window (see Figure 18). Select the **Scan removable drives** task from the list and press the **Run** button.

Immediately after you have launched the scan, a **Scanning** window will open (see Figure 5) displaying the progress while the action is performed with the objects selected from the list.

If you selected only one removable drive to be scanned, then after the scan is complete, Kaspersky Anti-Virus will suggest that you insert next disk.



Please pay attention to some peculiarities of the program.

- If you forgot to insert a CD or a floppy disk before you start the scan, or if the corresponding removable storage device, drive or the CD-ROM drive is disconnected, the scan will not be performed and the application will not display any additional message to notify you about it.
- If you inserted a floppy disk into the drive after the scan was started, the scan will not be performed. This rule also applies to CD-ROMs and other removable drives.
- After you took the floppy disk from the drive or disconnected the removable drive while the scan was in progress, the application will log an error message but will display no additional message. The application will proceed with scanning next removable drive (if any).

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

5.3. Processing malicious objects detected

The procedure used by Kaspersky Anti-Virus for processing detected dangerous objects, malicious software or objects possibly infected with viruses or their modifications, is fully dependent on the selected on-demand scan settings. This

section contains a discussion of cases when Kaspersky Anti-Virus offers various actions to be performed with the detected object during the scan or after the scan is complete.

Such situations take place when one of the following actions to be performed with the detected object was selected in the on-demand scan settings (see section 5.2.3.2 on page 54):

- **Prompt user for action during the scan.** Kaspersky Anti-Virus offers the user the choice of actions at the moment when such object is detected.

or

- **Prompt user for action once the scan is completed.** The user is prompted to select an action to be performed with dangerous objects only if you have initiated processing of such objects, that is, if you pressed the Process button in the window containing the scan results (see Figure 24).

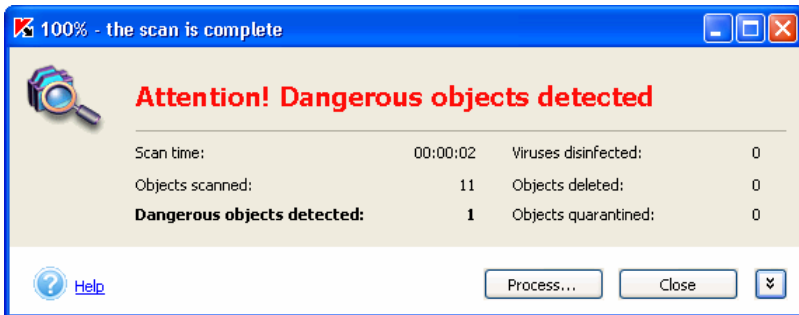



Figure 24. Delayed objects processing

Thus, upon detection of a dangerous object a message containing the following will be displayed (see Figure 25):

- a detailed description of the object with indication of the name of the malware detected;
- a set of actions that you can perform with the object. The set of the actions suggested will always contain one action recommended by the Kaspersky Lab's experts for processing the object. This action is marked by the word **(recommended)** next to it. You will be offered to perform one of the following actions (the set of actions suggested depends on the type of the object detected):

- **Disinfect** – attempt to disinfect the infected object if disinfection is possible. Before the first attempt to disinfect the object its copy will be saved to the backup storage.
- **Delete** – delete the infected or possibly infected object. When an object is deleted, its copy will be saved to the backup storage.
- **Skip** – perform no action with the object, only record information about this object in the report.



The dangerous object will be skipped if you close the window with notification about its detection using the  button in the top right corner.

- **Quarantine** – move object possibly infected with a virus or its modification to quarantine for the subsequent scan, restoration, sending to Kaspersky Lab for analysis or deletion.
- **Skip, add to exclusions** – add the program detected to the list of exclusions from the scope of the anti-virus scan and protection.



In order to use the exclusion you added, check the **Use general list of exclusions** box in the **List of exclusions** window.



Figure 25. Notification about detection of an infected object

You can also apply the selected action to all objects of this type by checking the corresponding box. Thus, for instance, in order to apply the selected action to all

infected objects that the application can disinfect, check box **Apply to all infected objects that can be disinfected within this session.**

If, for any reason, you decided against processing the objects by selecting the **Skip** option, you can return to their processing later. In order to do this press the [process these objects](#) link in the right section of the **Protection** tab. This will open the **Detected dangerous objects** dialog box (see Figure 26) that contains a detailed description of every dangerous object as well as the link to the corresponding description in the virus encyclopedia at www.viruslist.com.

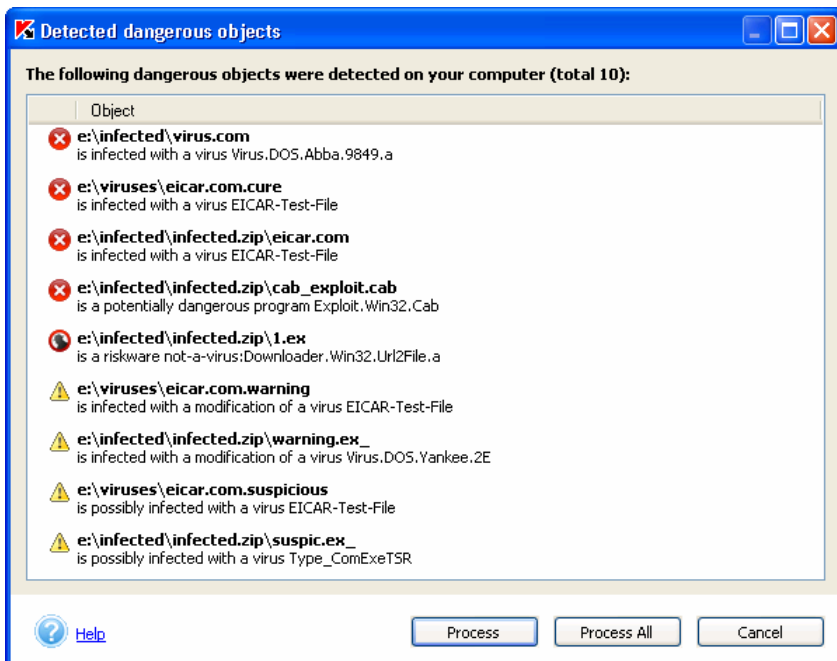


Figure 26. List of detected dangerous objects

You can process the object selected from the list by pressing the **Process** button or launch processing of all objects in the list by pressing the **Process All** button. As the result, the application will display messages (see Figure 25) that you can use to select an action to be performed with the object (a detailed description of possible actions see above).

In order to remove an object from the list without processing it, use the **Remove from the list** command of the shortcut menu (see Figure 27).

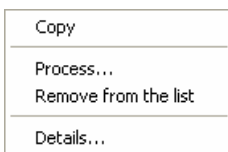


Figure 27. Shortcut menu of the **Detected dangerous objects** dialog box



If any of the dangerous objects has been deleted manually, it will be removed from the list of detected dangerous objects at the time of the attempt to disinfect it.

5.4. User's tasks

A list of system tasks is created during installation of Kaspersky Anti-Virus. The list includes both updating tasks (updating of anti-virus databases, updating application modules, databases rollback) and scanning tasks (full My Computer scan, automatic scanning on application launch, removable media scanning, and quarantine scan).

You can launch the system tasks by default and set up their parameters and schedule. Those tasks cannot be removed.



The process of setting parameters for the database and application component update tasks is described in section 5.1 on page 32. The task for rolling back the most recent updates has no specific settings.


While working with the Kaspersky Anti-Virus, administrators can create and manage tasks for scanning of custom objects.



Workstation users have no access to task creation and setup. They can view a list of tasks created by the administrator in the left frame of the **Protection** tab (see Figure 2) and run those tasks.

If you use remote administration of Kaspersky Anti-Virus, the list of tasks will include local and group tasks created using Kaspersky Administration Kit (see section 6.3 on page 116). Managing local tasks is similar to managing tasks created by the user: they can be launched, deleted, their settings can be modified. Group tasks cannot be launched or deleted, their settings cannot be modified; these tasks can be managed only via Kaspersky Administration Kit.



If modification of certain settings have been prohibited when managing tasks using Kaspersky Administration Kit (lock  has been set), then such tasks will not be available for editing via the local interface of Kaspersky Anti-Virus.



In order to create a new task,

use the **Create** button in the **On-Demand Scan tasks** window (see Figure 18). This will open a window (see Figure 19) that contains the following tabs: **Objects to be scanned**, **Settings**, **Schedule** and **Run on behalf of user's account**.

Enter the name of the task in the **Task name** field and configure all other settings (details see section 5.2.3 on page 48).

Settings of each task contain the **Display task on the "Protection" tab** box that controls task's display in the main application window. If the box is checked, the task will be visible to the workstation user in the left part of the tab and he or she will be able to run this task.

In order to remove an object from the list, select it and press the **Delete** button. However you have to remember that you can remove from the list only those tasks that were added manually. System tasks and group tasks created using Kaspersky Administration Kit cannot be deleted.

In order to run a task, select it from the list and press the **Run** button. This will open a window with information about the progress of the task execution.

In order to view the settings of the created task, select it from the list and press the **Properties** button.

5.5. Creating list of exclusions

Some situations require exclusions of some objects from the anti-virus scan scope. You can create such list of exclusions for tasks of on-demand scan.

The general list of all exclusions of anti-virus computer protection can be viewed and edited in special window **Threats and exclusions** (see Figure 14). In order to open this window follow [Threats and exclusions](#) link in the left section of the **Settings** tab (see Figure 3). The list of exclusions is created using the corresponding buttons.



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

As the result a window **Excluded object** (see Figure 28) will open where you can specify exclusions for Kaspersky Anti-Virus.

The following types of objects can be specified as exclusions:

- *Disks, folder, files, file masks.*

- *Threats* – types of malware and riskware;
- *Files related to specific threats* - specific files assigned certain types of threats after scanning.



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

fill in the **Object** field using button .

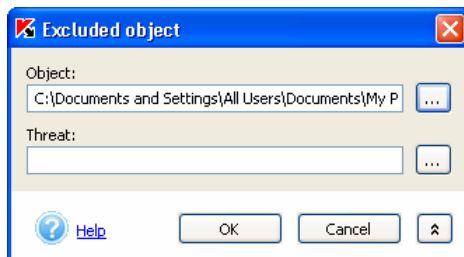


Figure 28. Creating a list of exclusions



When creating a path to the folder or to an object, that you would like to exclude from the scan scope, you can use the system environment variables. For example, you can exclude from the scan scope Microsoft Windows installation folder by specifying **%windir%** variable.



When adding objects using masks, you can enter several masks at the same time, in this case masks must be separated by a space. If a file name contains spaces, such names must be entered in double quotes.

Examples of legal exclusions masks:

- Masks the path to objects:
 - ***.exe** – all files with extension **exe**
 - ***.ex?** – all files with extension **ex?**, where **?** represents any single character
 - **test** – all files with filename **test**
- Masks with absolute paths to objects:
 - **C:\dir*.*** – all files in folder **C:\dir**
 - **C:\dir*.exe** – all files with extension **exe** in folder **C:\dir**
 - **C:\dir*.ex?** – all files with extension **ex?** in folder **C:\dir**, where **?** represents any single character

- **C:\dir\test** – only file *C:\dir\test*
- **C:\dir** – all files in folder *C:\dir* and all files in all subfolders of *C:\dir*
- Masks with relative paths to objects:
 - **dir*.*** – all files in all folders named *dir*
 - **dir\test** – all files named *test* in folders named *dir*
 - **dir*.exe** – all files with extension *exe* in all folders named *dir*
 - **dir*.ex?** – all files with extension *ex?* in all folders *dir*, where *?* represents any single character
 - **dir** – all files in all folders named *dir* and in all subfolders under such folders





We do not recommend to specify exclusions by entering mask **.** or *** as it is equivalent to disabling real-time protection altogether.



We do not recommend that you specify as an exception any virtual disk created based on the file system folder using the *subst* command. This is meaningless since during the scan Kaspersky Anti-Virus treats this virtual disk as a folder and consequently scans it.



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

open the additional part of the window (see Figure 28) by pressing  button and select a threat in **The list of detectable threats** window (see Figure 29) that opens by pressing  button.

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

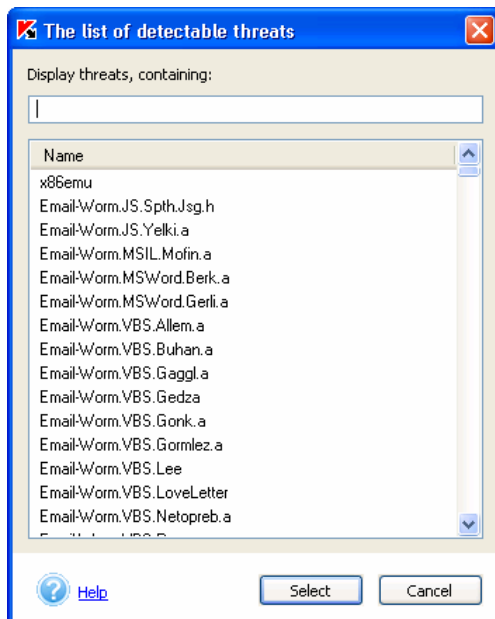


Figure 29. The list of detectable threats



In order to exclude a specific object of a known threat from the protection scope,

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



You can exclude a file of a certain type of threat using a notification message that opens when a file of this type is detected by Kaspersky Anti-Virus (see Figure 30). If you believe that this program is not dangerous and can be used in your computer, select the **Skip, add to exclusions** option. The program will be added to the list of exclusions from the scan scope in the **Threats and exclusions** window (see Figure 14).



Figure 30. Notification about a threat

5.6. Configuring schedule

You can create a schedule in order to automatically launch on-demand scan or updating tasks. This will allow timely updates of the anti-virus database and perform a regular anti-virus scan of your computer's objects based on this updated database.

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



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

1. Use the [Configure Updater](#) link in the left part of the **Settings** tab.
2. In the window that will open, select a task for which you need to create/modify the schedule and press the **Properties** button.

This will open an update settings window on the **Schedule** tab (see Figure 8).



In order to create/modify the on-demand scan task schedule,

1. Use the On-Demand Scan tasks link in the left section of the **Settings** tab.
2. In the window that contains the list of scan tasks (see Figure 18) select the task for which you need to create/modify the schedule and press the **Properties** button.

This will open a fine-tuning window for this task (see Figure 19). To configure the schedule switch to the **Schedule** tab (see Figure 31).

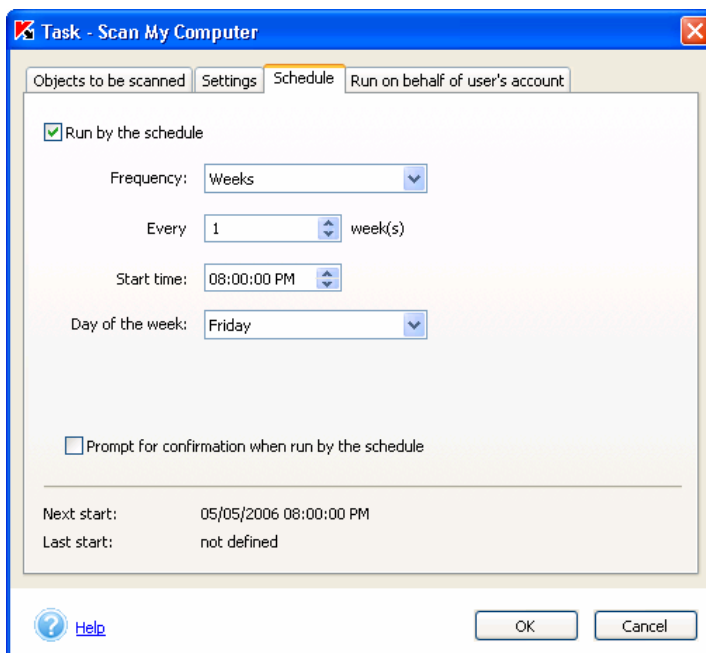


Figure 31. Creating a new task. The **Schedule** tab

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

If you would like to receive notifications about the updates about to be performed, check the **Prompt for confirmation when run by the schedule** box. If this box is checked, a **Scheduled task launch** window (see Figure 32) will be displayed on the screen before a scheduled scan task is launched. Press the **Start** button to start the scheduled scan. In order to postpone the scan for some time, select the required interval in the drop-down list and press the **Delay**

button. If the user takes no action in the prompt window within 3 minutes, the task will be started automatically.

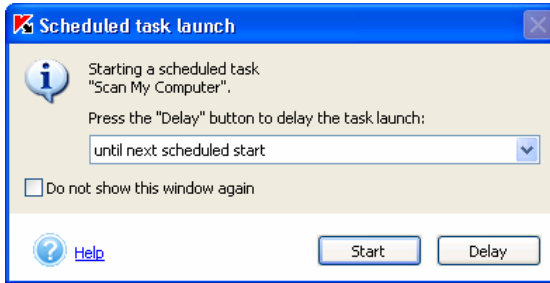


Figure 32. Prompt for launching a scheduled task

Use the **Frequency** field to define the periodicity for the task. The following options are available: *hours*, *days*, *weeks*, *at the program startup*. Depending upon the selected option, the central part of the window containing data input boxes will change its appearance:

- *Hours* – the task will run, in accordance with its schedule, every x hours. Define the frequency (in hours) as well as the date and time for the first launch.

Run by the schedule

Frequency: Hours

Every 1 hour(s)

Starting from: 13:44:02 January 12, 2006

Figure 33. Setting task schedule with hourly frequency

- *Days* – the task will run, in accordance with its schedule, every x days. Define the frequency (in days) and the time for the first launch.

Run by the schedule

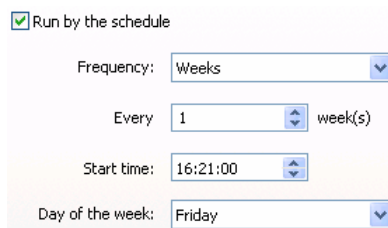
Frequency: Days

Every 1 day(s)

Start time: 16:21:00

Figure 34. Settings of task schedule with daily frequency

- *Weeks* – the task will run, in accordance with its schedule, every x weeks. Define the frequency (in weeks) and select the weekday and the time of task launch.



Run by the schedule

Frequency: Weeks

Every: 1 week(s)

Start time: 16:21:00

Day of the week: Friday

Figure 35. Setting task schedule with weekly frequency

- *At the program startup*: The task will be run immediately after opening of Kaspersky Anti-Virus.

5.7. Launching a task under a selected user's account

Kaspersky Anti-Virus includes the implementation of launching tasks by a user on behalf of a different account (impersonation).

By default this service is disabled and the tasks are launched on behalf of the current account. When this service is enabled, the administrator configures the account that has sufficient rights to access the object: for example, an on-demand scan task requires sufficient access rights for the object being scanned and an update task requires the right to access a local update folder or the rights of an authorized user of the proxy server.

This helps avoid a mistake when performing an on-demand scan task or an update task when the user, who initiated this task, does not have the required access right.

You can configure the launch of anti-virus tasks on behalf of a different account on the **Run on behalf of user's account** tab (see Figure 36).

In order to enable this server, check the **Run task under user's account**. By default the box is unchecked and the tasks are launched with the rights of the current account.

Using the field below enter the information about the account under which the task will be launched: username and password.

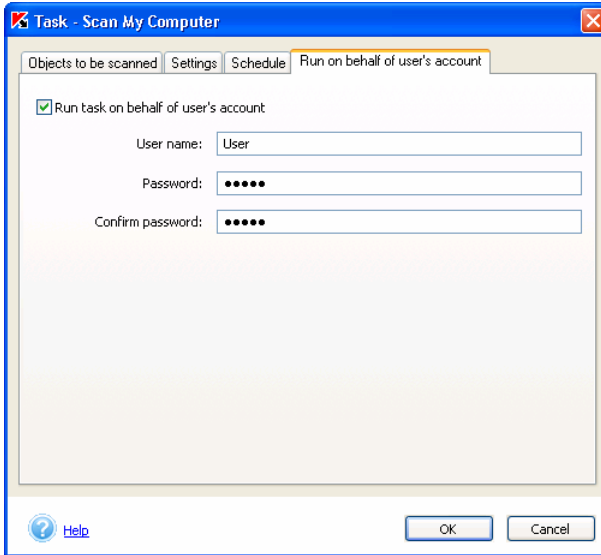


Figure 36. The **Run on behalf of user's account** tab

5.8. Additional features

Kaspersky Anti-Virus offers the following additional capabilities for product tuning and use, including:

- Working with suspicious objects relocated to quarantine storage.
- Working with backup copies of objects deleted or modified by Kaspersky Anti-Virus and located in the backup storage.
- Viewing of the application performance log.
- Managing Kaspersky Anti-Virus configuration
- Additional settings.
- Configuring prompts for confirmations

5.8.1. Quarantine and Backup storage

Kaspersky Anti-Virus gives users the option of isolating suspicious objects in quarantine or saving backup copies of infected objects in the backup storage prior to their disinfection or removal.

When a suspicious object is detected, the application isolates it in a quarantine directory, where the object can be rescanned, deleted, restored or sent to Kaspersky Lab for analysis.

The application creates a backup copy upon object detection before the first attempt of its disinfection or removal. This copy is saved to a backup directory, from which the object may be restored later if it contains valuable data.

5.8.1.1. Storage setup



In order to review or modify the settings for quarantine or backup storage,

use the [Configure Quarantine & Backup](#) hyperlink in the left frame of the **Settings** tab.

You can define the parameters for both storage directories using the tabs of the **Quarantine and backup storage settings** window.

In the window that will open (see Figure 37) edit the following settings for the quarantine and the backup storage on the corresponding tabs:

- Delete objects stored longer than (days):** By the maximum period for storage files in the quarantine is not restricted (the box is not checked). You can restrict the storage period by checking this box and specifying the required number of days in the entry field (the default suggested value is 90 days).
- Maximum size (MB):** By default the maximum quarantine size is not restricted (the box is not checked). If you would like to restrict the maximum total size of files located in the storage, check this box and enter the required value to specify the maximum size (the default value is 100 MB). Select the action that Kaspersky Anti-Virus will perform in case of the storage overflow:
 - *Notify user* – a notification with a prompt to select further actions will be displayed when the quarantine overflow occurs.
 - *Remove oldest objects* – delete files that had been quarantined at earlier dates compared to other quarantined files.
- Automatically scan quarantined objects every time the anti-virus database is updated.** This mode allows automatic scan of quarantined objects every time the database is updated without user's intervention.



Kaspersky Anti-Virus cannot scan quarantined objects immediately after your anti-virus database is updated if you are working with quarantine at the moment.

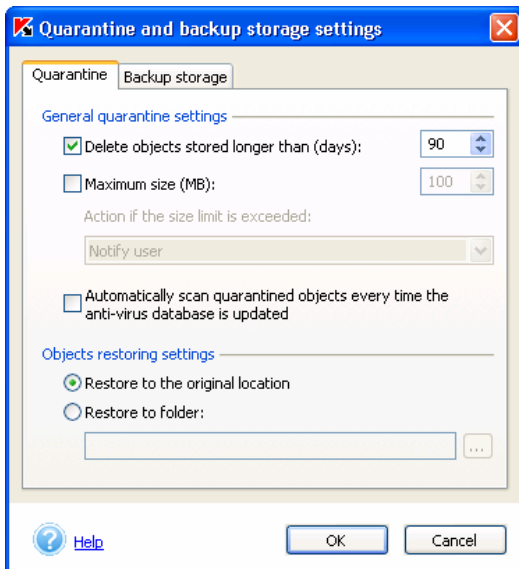


Figure 37. Configuring quarantine settings

Specify the location into which objects will be restored in the **Objects restoring settings** field:

- Restore to the original location.** By default the restored copy will be saved at the location where Kaspersky Anti-Virus had detected the original object.
- Restore to folder.** If you select this option, specify the path to the folder into which the restored objects will be saved.

The backup storage settings defining the maximum size, maximum storage period and backup copies restoration are analogous to the corresponding quarantine settings.

5.8.1.2. Work with Quarantine storage

Kaspersky Anti-Virus moves all suspicious objects detected during a full computer scan to quarantine, where you may continue operations with them (scanning, restoration, deletion, etc.)

By default Kaspersky Anti-Virus rescans quarantined objects after each update of its anti-virus database. If you need to check quarantined objects manually, we recommend updating the anti-virus database prior to such scan. Updated

databases may already contain information about viruses suspected in your files, in which case they might be disinfected.

Thus the work with suspicious files is performed in the **Quarantine** window (see Figure 38), which is opened by clicking the [View Quarantine](#) hyperlink in the **Protection** tab (see Figure 2) of the main application window or the [View Quarantine](#) hyperlink in the complete scan window (see Figure 5).



The **Protection** tab (see Figure 2) displays the total number of quarantined objects in brackets next to the [View Quarantine](#) link.

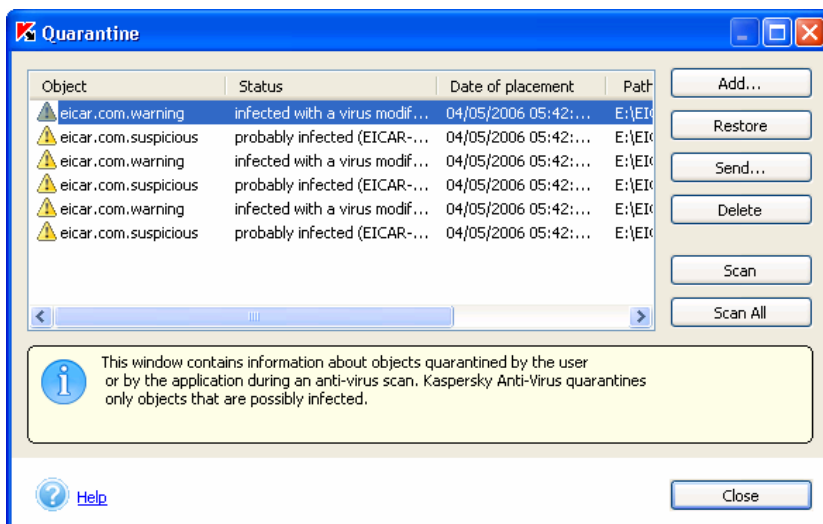


Figure 38. Quarantine window

In this dialog box, you can perform the following quarantine operations:

- Quarantine a file that you suspect of containing a virus even though it was not detected as such by Kaspersky Anti-Virus. In order to do this, press the **Add** button and select the suspicious file in the standard File select dialog box. This file will be added to the list with the *quarantined by user* status.
- Scan and disinfect all suspicious files or files selected from the list using the current anti-virus databases. In order to do this press the **Scan All** or the **Scan** button (after you have selected objects to be scanned).

Scanning and disinfection of any quarantined object may change its status to *infected*, *possibly infected*, *false alarm*, *not infected*, etc.

The *infected* status means that the object was identified as infected, but its disinfection has failed. We recommend deleting objects with this status.

All objects with the *false alarm* status can be restored with no reservation because their previous *possibly infected* status was not confirmed by Kaspersky Anti-Virus.



You can run the **Scan Quarantine** task of the **On-Demand Scan tasks** window (see Figure 18). A **Scan** window will open when the task is started (see Figure 5). You can view the scan results in the report.

The **Scan Quarantine** task is analogous to the task run by pressing the **Scan All** button in the **Quarantine** window (see Figure 38).

- Restore files to the same folders from which they were moved to quarantine. In order to restore an object, select it in the list and press the **Restore** button. During restoration of objects that had been quarantined from archives, mail databases and mail format files, you must additionally specify the folder into which they will be restored.



We recommend that you restore only objects with the false alarm, not infected or disinfected status, because restoration of other objects may result in a virus infection of your computer!

- Send suspicious objects to Kaspersky Lab experts for analysis. We recommend sending an object for expert analysis only in cases when its possibly infected status has not changed after several scans and disinfection attempts. In order to send the file for analysis press the Send button (details see Appendix A on page 156).



Please note that each file that you sent to Kaspersky Lab for analysis must be scanned with your Kaspersky Anti-Virus using the anti-virus database updated not earlier than one day before the file is sent.

- Delete any quarantined object or a group of selected objects. Delete only those objects which cannot be disinfected. In order to delete objects, select them in the list and press the **Delete** button.

5.8.1.3. Working with Backup storage

Kaspersky Anti-Virus creates a copy of an infected or suspicious object before attempting its disinfection or removal; the copy is saved to the Backup storage directory.

When necessary, you can restore any object if, for instance, its disinfection resulted in data loss, if the object has been erroneously deleted, or if you plan to reattempt its disinfection using the updated anti-virus databases.

Backup copies are operated on in the **Backup** window (see Figure 39), which opens after clicking the [View Backup](#) hyperlink in the **Protection** tab (see Figure 2) of the main application window.



The **Protection** tab (see Figure 2) displays the total number of objects' backup copies in brackets next to the [View Backup](#) link.

You can perform the following actions in the Backup storage window:

- Restore objects to the original directories from which they have been added to Backup storage or to a specified destination folder. In order to restore an object, select it from the list and press the **Restore** button.

The object will then be restored from the backup copy with the original name it had before the disinfection attempt.

If an object with the same name already exist in the original location (this situation is possible when you are restoring an object a copy of which had been created before the disinfection attempt), a corresponding warning message will be displayed. You can change the location for saving the object being restored or rename this object.

- Remove any file or a group of selected files from the storage. In order to delete a file, select it from the list and press the **Delete** button.

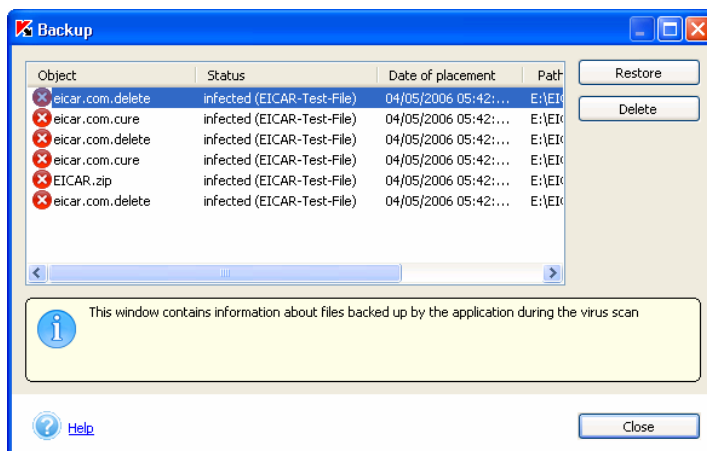


Figure 39. Backup storage window

When can I restore backup copies?

Sometimes, during disinfection of an object its integrity cannot be preserved. If the disinfected file contained important information that became partially or completely unavailable after disinfection, you can try to restore the original object from its backup copy. We recommend performing anti-virus scan of the object immediately after it has been restored. Using the updated anti-virus database the application may be able to disinfect it without breaching its integrity.



We do not recommend restoring backup copies of objects unless it is absolutely necessary. This may result in a virus infection of your computer.

By default the maximum backup copies storage period and the maximum size of the backup storage are not restricted. We recommend that you view and clean the backup storage on a regular basis. You can setup the program in a way so that it automatically deletes older copies and notifies you when the storage overflow occurs (see section 5.8.1.1 on page 73).

5.8.2. Working with reports

During the execution of the full computer scan and of the anti-virus database updating the application creates reports about objects scanned and the results of processing of such objects that also include general statistical information.

Kaspersky Anti-Virus maintains a complete report on the results of all completed tasks in the **Reports** window (see Figure 40), which can be reviewed by clicking the [View reports](#) hyperlink in the left frame of the **Protection** tab (see Figure 2). Here is where it records the status of each task, together with the date and time of its completion.



Figure 40. The **Reports** window

The status information about object processing may belong to one of the following categories:

- ▶ or ⓘ *Information report* contains reference information (for example: *task started*, *task completed*, *task running*, *task paused*).
- ✖ *Attention report* includes critical information (for example: Attention! Some objects remained unprocessed).
- ⚠ *Note report* contains comments about some important moments in the applications' operation (for example: task interrupted).

As a rule, notifications of success and informational messages are for reference only and thus they are not of critical importance. You can disable the display of task reports which contain only those message types. In order to do so, uncheck the **Show information reports** box. Please note that reports about execution of a specific task marked with ▶ icon will always be displayed.

This window also enables you to sort provided reports by the type, name (in the alphabetical order), or by completion time of the task reported. In order to sort reports listed in the window by any of the above types, simply left-click on the heading of the corresponding column.

You can perform the following actions in this window using the shortcut menu (opens by left-clicking the report name):

- **Export detailed report to file** Using a standard Microsoft Windows dialog box that will open enter the file name, select a disk folder into which this file will be saved and press the **Save** button. The report will be saved in the Microsoft Excel table or in the text format.
- **Send report to Kaspersky Lab.** You can send this report if the task (for example a computer scan or anti-virus database update) was interrupted or resulted in an error and you do not know the reason for this behavior of the application. This will automatically open your default mail client program, for example, Microsoft Outlook Express with a new message with the report file attached to it. Send this letter and the Kaspersky Lab's specialists will try to help you as soon as possible.



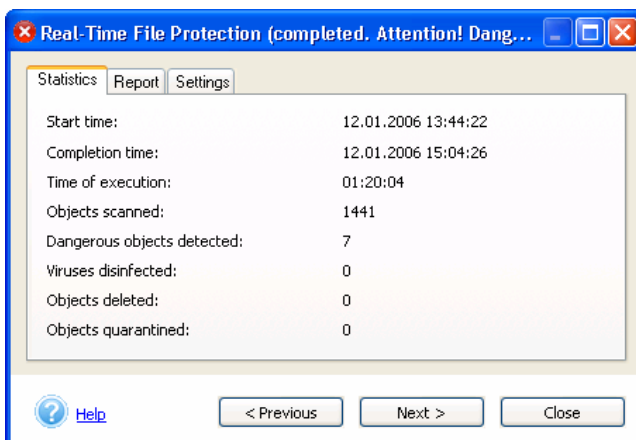
Automatic creation of e-mail messages is always performed in Microsoft Office Outlook or Microsoft Outlook Express. If you have a different e-mail system (for example, The Bat!) installed on your computer, you will have to configure Simple MAPI support for this program to automatically create e-mail messages.

You can delete one or all of the reports from the list by using the **Delete report** or **Delete all reports** command. You cannot delete a report related to a task currently in progress.

You can review the settings, statistics and a report on detected objects for any task using the respective tabs if you select it in the log. Click the **Details** button to accomplish this.

Clicking the button will open a window containing a detailed report about task performance represented by the **Statistics**, **Report** and **Settings** tabs.

Thus, the **Statistics** tab (see Figure 41) lets the user review the general information about the work performed by Kaspersky Anti-Virus to complete the task: the date and time of task start and its completion, the total number of scanned files, and the number of infected, disinfected, and quarantined objects. When the updating task is running, the tab will display the total size of updates at the update source and the size of updates downloaded to your computer.

Figure 41. The **Statistics** tab

By default the **Report** tab (see Figure 43) does not contain information about “clean” objects and will display only information about detected viruses. In order to display information about clean objects, check the **Log all reports** box in the additional settings of Kaspersky Anti-Virus (see section 5.8.4 on page 83). In this case the tab will display information about all objects scanned. For the updating tasks this tab contains information about each step of this task: establishing connection to the updates sources, files downloaded and information about their installation on the computer. Information on this tab is always displayed irrespective of whether the **Log all reports** box in the additional settings of Kaspersky Anti-Virus is checked.



*If you do not wish the application to display information reports within the current session and you do not wish to uncheck the **Log all reports** box,*

while viewing reports on the **Report** tab (see Figure 43), right-click to open the shortcut menu (see Figure 42) and uncheck the **Show detailed report** box.

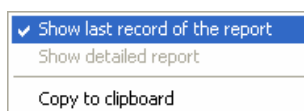
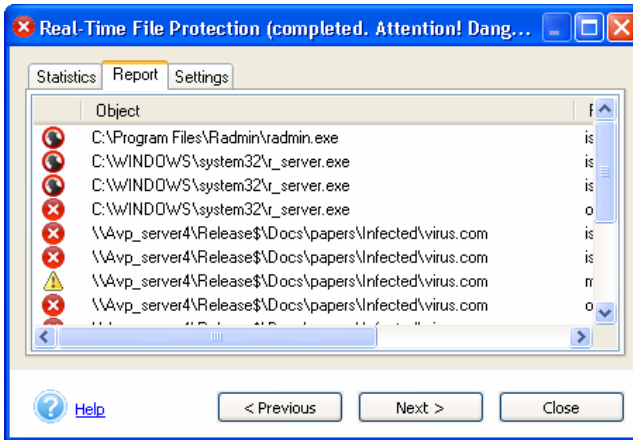


Figure 42. Report shortcut menu

You can also copy information about individual events into the clipboard. In order to do this, select the event you need and use the **Copy to clipboard** command from the shortcut menu.

Figure 43. The **Report** tab

The **Settings** tab (see Figure 44) displays the task settings. This tab contains information about the objects scanned, scan level selected for this task and actions to be performed by the application with the infected objects, malware and possibly infected files.

Figure 44. The **Settings** tab

You can select the tasks for review either in the Task Log or directly in the detailed report window using the **Next** and **Previous** buttons or by clicking the task name in the respective drop-down list.

You can configure the settings for the reports log in the **Additional settings** window (see Figure 46), which is displayed after clicking the corresponding hyperlink in the left frame of the **Settings** tab (please see details in section 5.8.4 on page 83). Here you can define the maximum duration for storing reports and enable/disable inclusion of informational messages to the detailed report.

5.8.3. Managing Kaspersky Anti-Virus configuration

Kaspersky Anti-Virus allows you to create and use various configuration of its operation. Now you can configure a certain application operation mode, save its settings into a special configuration file, called a *profile*, and use this configuration whenever you need.

In order to switch to managing the application's configuration, use the [Managing profiles](#) link in the left section of the **Settings** tab (see Figure 3).

Using the window that will open (see Figure 45), by pressing the **Save profile** button you can save the current application settings in a special configuration file or by clicking the **Load profile** button – apply settings of a configuration file created earlier to the operation of Kaspersky Anti-Virus.

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

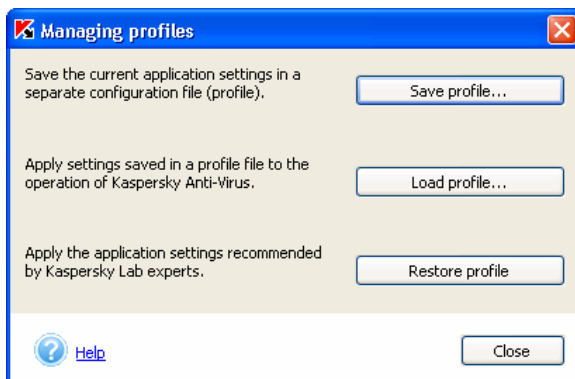


Figure 45. Managing profiles

5.8.4. Additional settings

Apart from configuring settings of specific tasks, Kaspersky Anti-Virus also allows configuring various common and service settings (see Figure 46).



In order to configure additional settings of Kaspersky Anti-Virus,

Use the [Additional Settings](#) link in the left section of the **Settings** tab (see Figure 3). This will open a window that contains tabs **General**, **Efficiency** and **Security**.

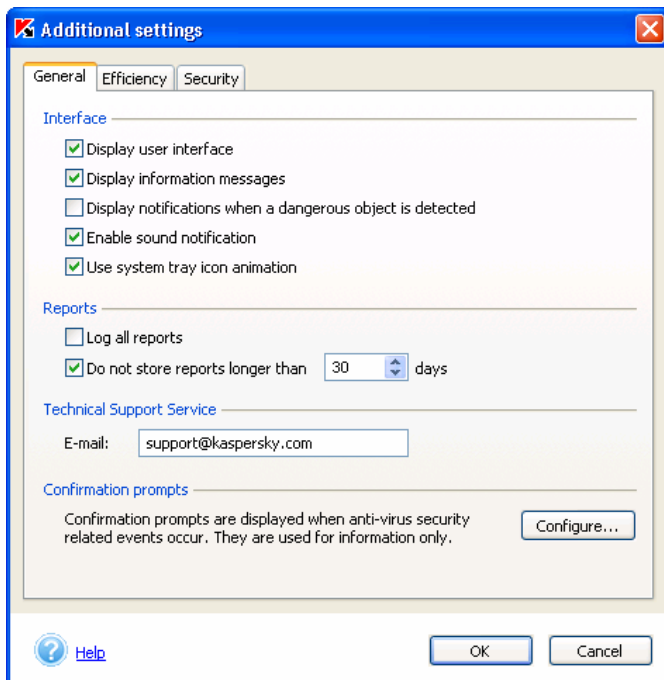


Figure 46. Additional settings of Kaspersky Anti-Virus.
The **General** tab

You can perform the following using the **General** tab (see Figure 46):

- Display user interface** – enable the display of the application icon in the system tray and enable starting the main application window in the user's mode (see 5.8.7 on page 89).



User interface display settings will be applied only after the computer restart.

- Display information messages** – allow displaying all messages accompanying the operation of Kaspersky Anti-Virus. The messages will appear above the application icon in the system tray.



Display of information messages is not available if you are running Microsoft Windows 98 or Microsoft Windows NT Workstation 4.0 operating system.

- Display notifications when a dangerous object is detected** – enable displaying information messages about detection of dangerous objects.
- Enable sound notification** – enable sound effects for events occurring during the operation of Kaspersky Anti-Virus. You can view the list of events and change the set of sound files corresponding to these events using the standard Microsoft Windows tools (**Start → Settings → Control Panel → Sounds and Audio Devices → Sounds**).
- Use system tray icon animation** – enable animation of the icon depending on the operation being performed by Kaspersky Anti-Virus. For example a blinking envelope icon appears when an e-mail message is being scanned.
- Log all reports** – enable logging of all reports generated during the application's operation: information messages, error messages, etc. By default this mode is disabled – only important reports will be logged, such message notifying that the application operation completed with an error, or a task was interrupted, etc.
- Do not store reports longer than ... days.** The default reports storage period is 30 days. You can edit the storage period by entering the desired value into the field to the right of the checkbox or by unchecking this box. A check for reports stored longer than the specified storage period will be performed and obsolete reports will be deleted at Kaspersky Anti-Virus startup.

You can specify the address of the Technical Support service in the **Technical Support Service** section. By default the e-mail address of the Kaspersky Lab's Technical Support service is used: (support@kaspersky.com). Using this field you can specify, for example, the security administrator's address or a URL that will open when you request support.

The **Confirmation prompts** section allows you to define whether notifications about some events in the operation of Kaspersky Anti-Virus will be displayed. As a rule, all notifications are provided for reference only. Details about configurations of confirmation prompts see section 5.8.5 on page 88).

You can configure restrictions to be imposed to the on-demand scan in order to save the battery (if you are using a notebook computer) and the operating systems' resources (details see section 5.8.6 on page 89) on the **Efficiency** tab (see Figure 47).

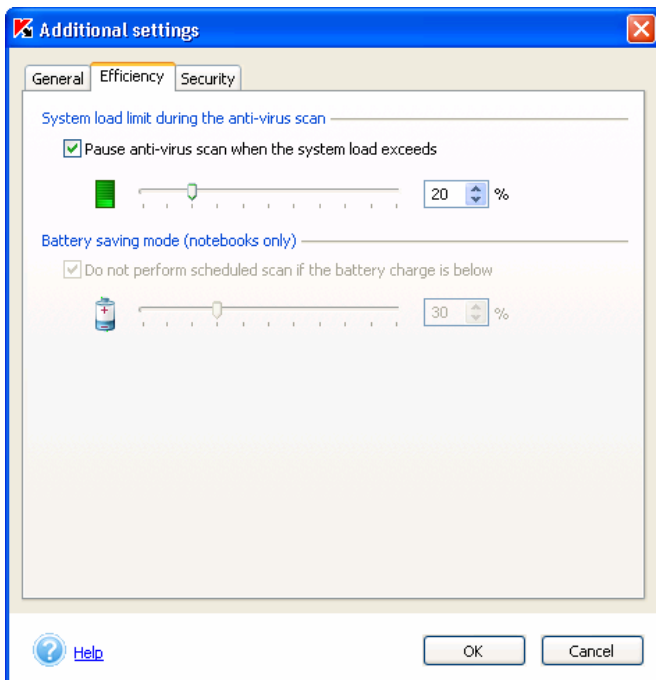


Figure 47. Additional settings of Kaspersky Anti-Virus
The **Efficiency** tab

The **Security** tab (see Figure 48) contains the following settings:

- Launch Kaspersky Anti-Virus at the system startup** – enable Kaspersky Anti-Virus launch after the operating system startup.



Figure 48. Additional settings of Kaspersky Anti-Virus
The **Security** tab

- Use recovery after errors system** – enable Kaspersky Anti-Virus operation recovery system in case of a failure during its operation. If an error occurred during the operation of the application, then the main application window of Kaspersky Anti-Virus will minimize (if it was opened) and an information message will appear above the system tray icon (see Figure 49). After this the application’s operation will be recovered.

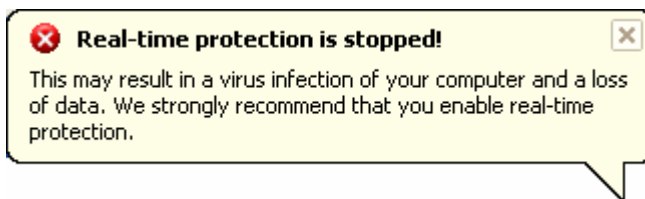


Figure 49. Operation error.

- ✔ **Use password for application protection** – enable prompt for password when switching to the administrator's mode. We recommend using this mode if there is another user (or users) who has access to your computer and you do not wish him or her to change the anti-virus protection settings or close Kaspersky Anti-Virus (details see section 5.8.7 on page 89). When enabling this mode, enter the necessary number of characters in the **Password** field and re-enter these characters in the **Confirm password** field.

5.8.5. Configuring prompts for confirmation

If you would like to be notified about certain events occurring during the operation of Kaspersky Anti-Virus, follow the [Additional Settings](#) link in the left section of the **Settings** tab (see Figure 3). In the additional settings configuration window that will open, press the **Configure** button in the **Confirmation prompts** section. By doing this you will switch to a dialog box where you can configure prompts for confirmation (see Figure 50).

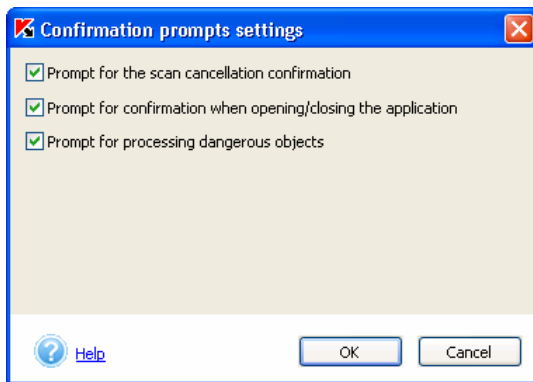



Figure 50. Configuring prompts for confirmation

The following events can be associated with prompts for confirmation:


- ✔ **Prompt for the scan cancellation confirmation** – display a prompt or confirmation when canceling an on-demand scan. If the scan was cancelled a pop up message containing explanation of the reasons why the scan was cancelled will appear above the system tray application icon.
- ✔ **Prompt for confirmation when opening/closing the application** – display a prompt for confirmation when opening/closing of Kaspersky Anti-Virus.

-  **Prompt for processing dangerous objects** – display a warning to notify user that some infected objects remained unprocessed after the virus scan.

5.8.6. Restricting efficiency of Kaspersky Anti-Virus


You can impose restrictions on the on-demand scan launch if you feel that it is necessary to save the use of your computer's resources. In order to do it, follow the [Additional Settings](#) link in the left section of the **Settings** tab (see Figure 3). In the additional application settings window that will open, switch to the **Efficiency** tab (see Figure 47).

You can impose the following restrictions:

-  **Pause anti-virus scan when the system load exceeds ...%** – pause the on-demand anti-virus scan if the file system load is above the specified level. Once the file system load decreases to the allowable level, the scan will be resumed. Using a slider or the entry field to the right of the setting specify the allowable file load level (in percents) above which scheduled scans cannot be started.



This setting applies only to the on-demand scans (for example, to the scan of selected objects). Real-time anti-virus protection will not be affected.

-  **Do not perform scheduled scan if the battery charge is below -** cancel scheduled scans if you are using a laptop computer if the battery charge is below the specified value. Using a slider or the entry field to the right of the setting specify the allowable battery charge level (in percents) below which scheduled scans cannot be started.



This setting is available only if Kaspersky Anti-Virus is installed on a laptop computer powered from a battery.

5.8.7. Working in the administrator's and the user's mode

Kaspersky Anti-Virus can operate in two modes: the administrator's mode and the user's mode. The use of these modes may be convenient if there is another user who has access to your computer. You can prevent this user from changing the anti-virus settings or closing Kaspersky Anti-Virus. In the user's mode the

application interface will change and unavailable settings will be hidden (for example, the **Settings** tab will not be displayed in the main application window).

You can enable the use of the user's and administrator's modes using the local interface or the Kaspersky Administration Kit application (see section 6.2.2.8 on page 111).



In order to enable the use of the user's and the administrator's modes using the local interface,

Check the **Use password for application protection** box on the **Security** tab (see Figure 48) in the Kaspersky Anti-Virus additional settings window. Enter the password in the **Password** field and re-enter it in the **Confirm password** field.

As the result the **Switch to user mode** command will appear in the shortcut application menu (see Figure 1). You can use this command to switch to the user's mode. In order to return to the administrator's mode, use the **Switch to administrator mode** command from the shortcut menu and enter the password in the dialog box that will open (see Figure 51).



If the **Use password for application protection** box (see Figure 48) is not checked, Kaspersky Anti-Virus will open and operate in the administrator's mode.



Figure 51. Entering password



In order to hide the application interface completely while the application is in the user's mode,

uncheck the **Display user interface** box on the **General** tab (see Figure 46) in the Kaspersky Anti-Virus additional settings window.

In this case the Kaspersky Anti-Virus application icon will not be displayed in the system tray and the main application window will not open.

CHAPTER 6. MANAGING THE APPLICATION USING KASPERSKY ADMINISTRATION KIT

6.1. Managing installation packages

This section contains information about creation and configuration of an installation package for Kaspersky Anti-Virus 5.0 SOS. More detailed information about managing installation packages see the Kaspersky Administration Kit 5.0 Administrator's Guide.

6.1.1. Creating an installation package



In order to create an installation package, perform the following:

1. Connect to the Administration Server.
2. Select the **Remote installation** node in the console tree, open the shortcut menu and select the **New/Installation Package** command or use the analogous item from the **Action** menu. This will launch the wizard. Follow its instructions.

The policy creation application is designed as a Microsoft Windows wizard (Windows Wizard) and includes a sequence of windows (steps). To switch between the wizard dialog boxes, use **< Back** and **Next >**. To finish working with the wizard, click **Finish**. To cancel the wizard at any stage, click **Cancel**.

During creation of the installation package the minimum set of settings is configured. Other values are set by default and correspond to the default values used for the local installation of the application. You can modify the installation package settings by editing them (see section 6.1.2 on page 94).

Step 10. Entering the name of the installation package

First windows of the wizard and used to entering data. Here you will have to specify the name of the installation package (field **Name**).

Step 11. Connecting the installation package description file

Specify the application to be installed in the next window of the wizard (see Figure 52). Select option **Make Kaspersky Lab's application package** from the drop-down list and using the **Browse** button select the file containing description of the application (this file has extension **.kpd** and is included into the distribution package of Kaspersky Anti-Virus 5.0 SOS). As the result, the fields with the application name and the version number will be filled automatically.

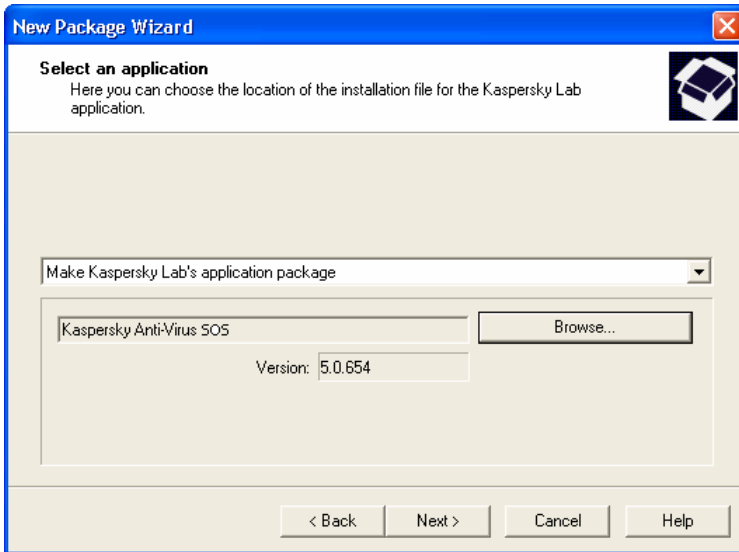


Figure 52. Creating an installation package Selecting application to be installed

Step 12. Selecting the license key file

In the next wizard window (see Figure 53) you can specify the license key that will be included into the installation package. In order to do it press the **Browse** button and select the required license key file (a file with the **.key** extension).

If you do not wish to include a license key into the structure of the installation package, simply press the **Next** button.

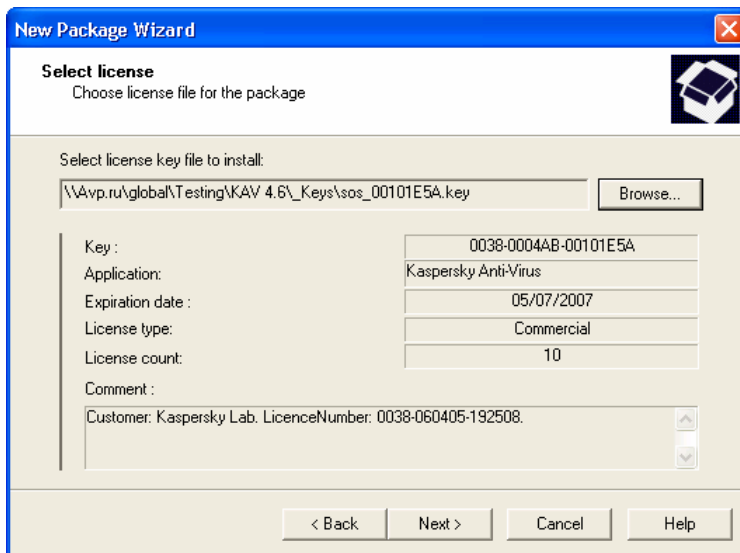


Figure 53. Creating an installation package. Selecting the license key file

Step 13. Completing the creation of an installation package

Press the **Next** button in the **Loading the installation package** window.

After this the set of files required for the installation of the specified application onto the client computers will be loaded into a public folder of the Administration Server and a check will be performed to determine whether the administration plugin for the selected application is installed on the administrator's workstation. If the plugin is not installed or if it is of an earlier version compared to that included into the distribution package, it will be installed or the older version will be replaced.

The next wizard window will display information about the successful completion of the installation package creation process. As the result the created installation package will be added to the **Remote installation** mode and displayed in the results pane.

6.1.2. Viewing and editing the installation package settings



In order to view and/or edit the values of the installation package settings:

1. Select the installation package whose settings you wish to edit in the **Remote install** package of the console tree.
2. Open the shortcut menu of the selected policy and use the **Properties** command to display the policy **Settings** window for **Kaspersky Anti-Virus 5.0 SOS**, that contains several tabs.

This will open a **<Installation package name> Properties** window that consists of the following tabs: **General**, **Installation settings**, **License info** and **OS reboot**.

The **General**, **Licenses** and **Operation System restart** tabs are standard tabs for the Kaspersky Administration Kit application (details see Kaspersky Administration Kit 5.0 deployment manual).

The **Installation settings** tab (see Figure 54) contains the following settings of Kaspersky Anti-Virus 5.0 SOS:

- Client computer application **Installation folder**. If the field is left blank, the installation will be performed into the default folder: **<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 5.0 SOS**.
- **Uninstallation password** – password that will be asked for when you attempt to uninstall the application. Enter the password in the corresponding field and re-enter it in the **Confirm password** field.
- **Password for application protection** – password for switching between the user's and the administrator's mode. Enter the password in the corresponding field and re-enter it in the **Confirm password** field.

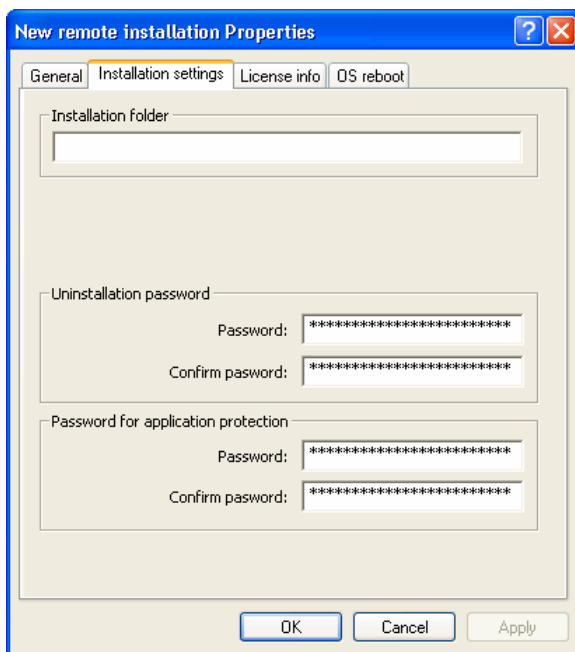


Figure 54. Installation package properties. The **Installation settings** tab

6.2. Managing policies

This section describes how to create and manage policies for Kaspersky Anti-Virus SOS. Detailed information about managing policies see the Administrator's Guide for Kaspersky Administration Kit 5.0.

6.2.1. Creating a policy




To create a new policy, perform the following actions:

1. In the **Groups** node of the console tree, select a group of computers to be assigned the new policy.
2. Select the **Policies** folder within the selected group, open the shortcut menu, and click **New → Policy...** to begin a wizard for creating a new policy.

The application for creating a new policy is organized as a Microsoft Windows Wizard which will guide you through the process. To switch between the wizard dialog boxes, use **< Back** and **Next >**. To finish working with the wizard, click **Finish**. To cancel the wizard at any stage, click **Cancel**.

During the step of creating a policy, the minimum set of settings will be configured without which the application will not work. Other values will be set by default and will correspond to the default values for the local installation of the application. You can change the policy by editing it (see 6.2.2 on page 99).



During policy creation (Step 1 – Step 4) you can prohibit modification of settings in the policies of nested groups, in application and task settings. To disable the modification of settings "lock" them up: .

The settings allowed for modification will be marked with .

Step 1. Entering general information about the policy

The first wizard dialog boxes are introductory steps, where you should enter the policy name into the **Name** field and select the **Kaspersky Anti-Virus 5.0 SOS** product from the **Application name** drop-down list. If you want the policy you are creating as the active policy for the application, activate the policy by checking the **Activate the policy** box in the corresponding dialog box of the wizard.



You can define several policies with different settings values in a group for one application. However, there can only be one current policy for the application. You can activate a policy which is not currently active policy, by an event which allows establishing stricter anti-virus protection settings in the period of virus outbreaks.

Step 2. Define the anti-virus protection level for on-demand scanning

In this dialog box, define the anti-virus protection level for the new policy (see section 4.2 on page 29), which will be used while running the on-demand scanning tasks and specify actions to be performed when an infected or a suspicious object is detected (see section 5.2.3.2 on page 54).

Clicking the **Details** button opens a window containing advanced settings for the on-demand scanning mode (see Figure 59). If you modify any of the predefined level settings, the level of anti-virus protection will change to **Customized**.

Step 3. Select the update source

During this stage (see Figure 55), you will be asked to set up the parameters for updating the anti-virus database and application modules. You will have to specify the source of updates and define network settings in the window which opens after clicking the **LAN Settings** button. All settings are identical to local setup. Detailed information on this issue can be found in section 5.1.3 on page 34.

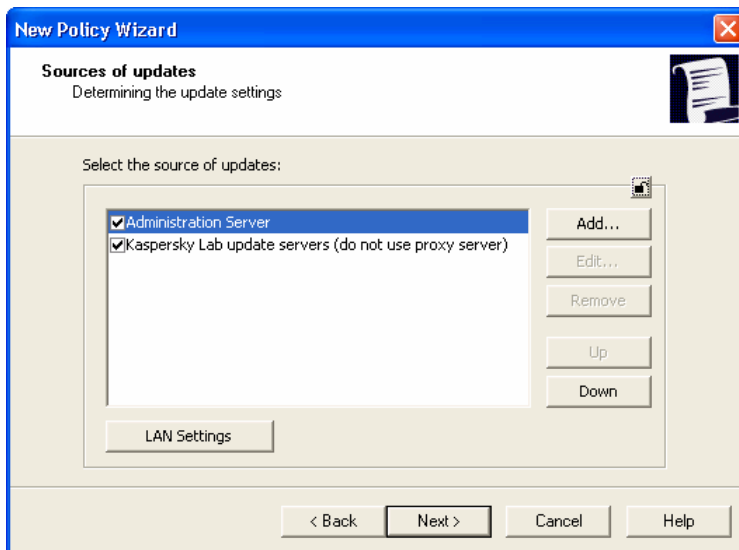


Figure 55. Selecting the update source

Step 4. Define updating parameters

In this dialog box (see Figure 56), you can select the settings of the update service for the application modules. Settings of the updating procedure are identical to local setup. Detailed information on this issue can be found in section 5.1.3 on page 34.

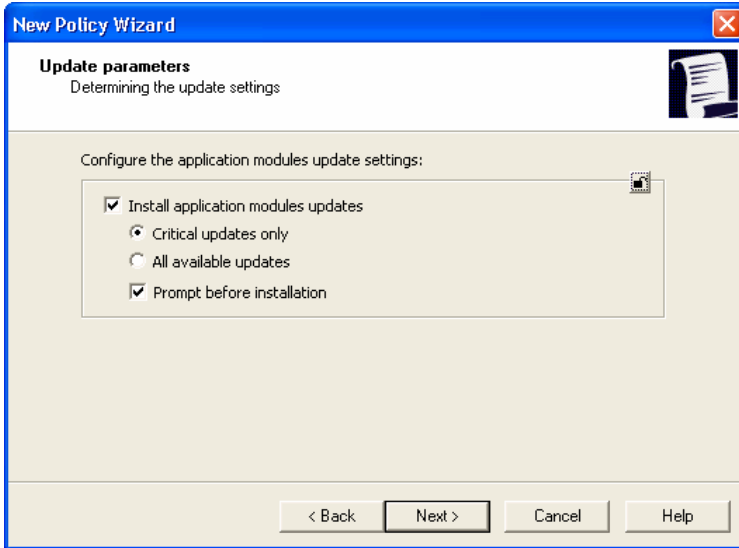


Figure 56. Selection of the update service parameters

Step 5. Completing creating the policy

The final window of the wizard informs you that a new policy has been successfully created.

After the wizard is closed, the policy for this application will be added to the **Policies** folder of the corresponding group and shown on the results panel.

To apply the policy, edit its settings and specify restrictions for modification of task settings and application settings if you have not done so during policy creation. The policy will be applied to client computers upon the first synchronization of the clients with the Administration server.


A policy is applied as follows: currently running periodic tasks, such as on-demand scanning or updating, will continue with old settings. In this case, the changes will be applied the next time the application starts.

You can copy and move policies from one group to another and handle the policies using the standard commands in the shortcut menu, such as **Copy/Paste**, **Cut/Paste**, and **Delete**, or analogous commands in the **Action** menu. To relocate a policy, drag the policy icon with your mouse to another location.

6.2.2. Viewing and editing policy settings

At the editing stage, you can customize policy settings, prohibit changes in the policy settings for nested groups, and lock application and task settings so that users cannot modify them.



To lock the configuration settings so that users cannot change them, mark them with the “lock” icon: . The settings that can be changed are marked as .



To view the current policy settings and / or change them:

1. In the **Groups** folder of the console tree, select a group of computers for which you want to change policy settings.
2. Select the **Policies** folder in this group. All policies available for this group will be displayed on the results panel.
3. In the list of policies, point to a policy for **Kaspersky Anti-Virus 5.0 SOS**. (the application name is displayed in the **Application** field).
4. Open the shortcut menu for the selected policy and click **Properties**. You will see a window with the policy properties for **Kaspersky Anti-Virus 5.0 SOS**, containing several tabs.

The **General**, **Enforcement**, and **Event processing** tabs are standard Kaspersky Administration Kit tabs (details see the Kaspersky Administration Kit 5.0 Reference Guide t).

The remaining tabs display specific settings for Kaspersky Anti-Virus 5.0 SOS.. These tabs are described in more detail below.

6.2.2.1. Viewing information about policy

The **General** tab (see Figure 57) displays the general information about the policy:

- Policy name;
- The application this policy is assigned to (**Kaspersky Anti-Virus 5.0 SOS**);
- Application version;
- Date and time of creation;
- Date and time of the last modification.

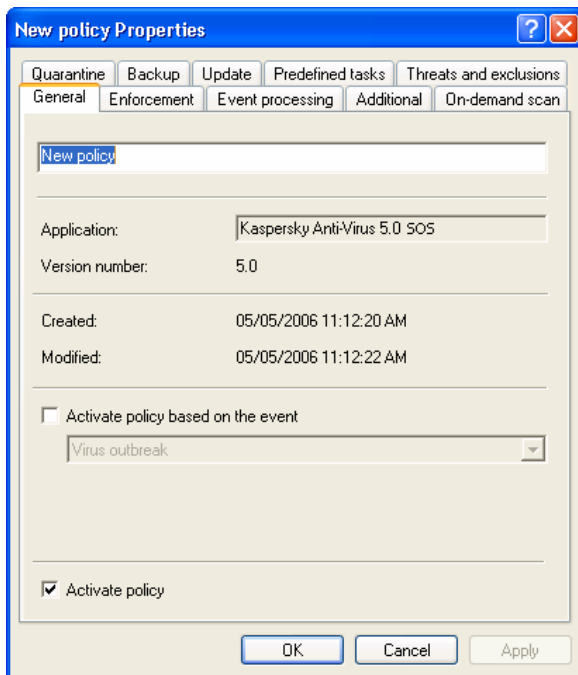


Figure 57. The **General** tab

On this tab, you can edit the policy name.

If you wish to make the policy active, check the **Activate policy** box. If you would like to activate the policy automatically on the occurrence of a certain event, check the **Activate policy based on the event** box and select from the drop-down list the event you need. You can return to the previous policy only manually.

6.2.2.2. On-demand scanning

To configure policy settings for on-demand scans use the **On-demand scan** tab (see Figure 58).

Select one of the three predefined levels of anti-virus security from the drop-down list in the **Protection level configuration** section (see section 4.2 on page 29).

You can specify the type of action to be performed when an infected or suspicious object is detected in the **Actions to be performed with detected objects** section (details about the type of actions performed by Kaspersky Anti-Virus in the on-demand scan mode, see section 5.2.3.2 on page 54).

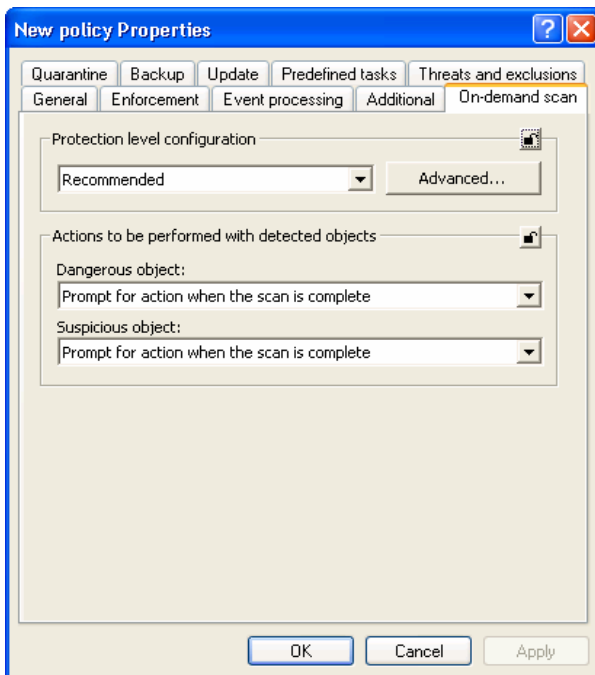


Figure 58. The **On-demand scan** tab

The **Configure on-demand scan** window is opened by clicking the **Advanced...** button. Using this window you can view the settings corresponding to the selected level or configure your own settings based on the existing settings. In this case the protection level will change to **Customized**.

The advanced settings window contains the **Scan scope** and **Additional** tabs.

Use the **Scan scope** tab (see Figure 59) to specify the objects to be scanned, define their type and a list of those to be excluded from scanning (for details see section 5.2 on page 43).

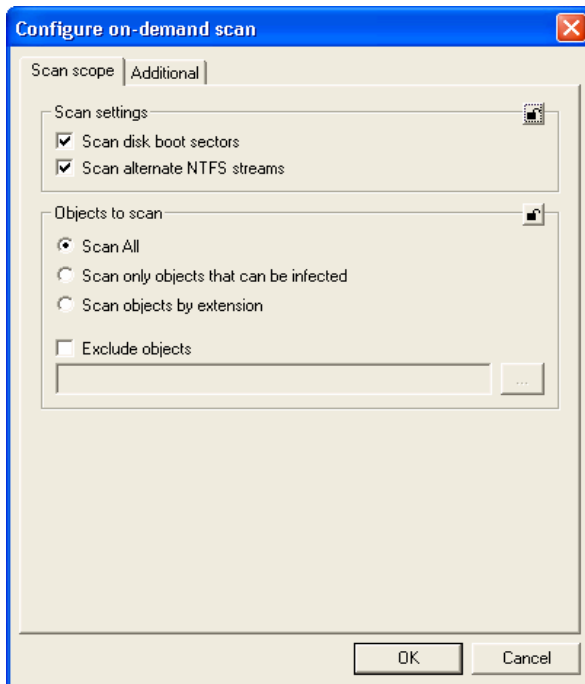
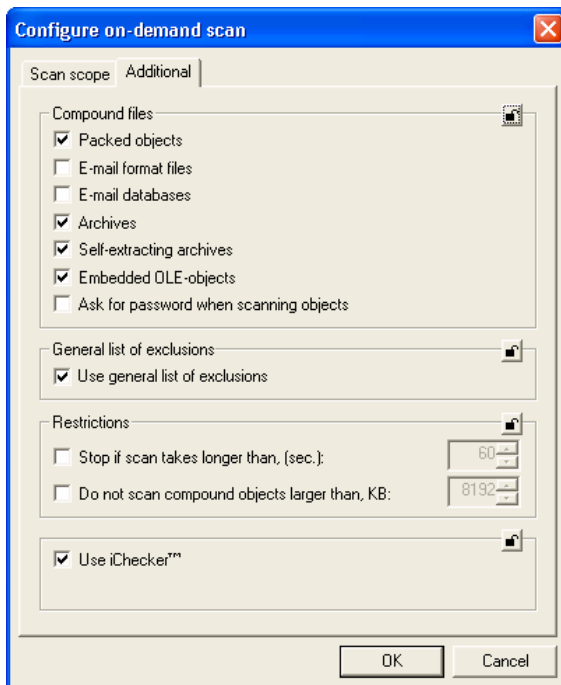


Figure 59. The **Scan scope** tab

Within the **Additional** tab (see Figure 60) you can enable/disable scanning for various types of composite files, exclude allowed potentially dangerous programs from the scope of the scan and enable output of a password prompt for encrypted archives or specify certain restrictions for the scanning process (for details see section 5.2 on page 43).

Figure 60. The **Additional** tab

6.2.2.3. Threats and Exclusions

You can use the **Threats and exclusions** tab (see Figure 61) to specify the type of the anti-virus database (standard or extended) to be used for the scans and to create a list of exceptions from the scan scope. These settings are similar to the settings of the local interface (details see section 5.1.3.5 on page 42 and section 5.5 on page 64).

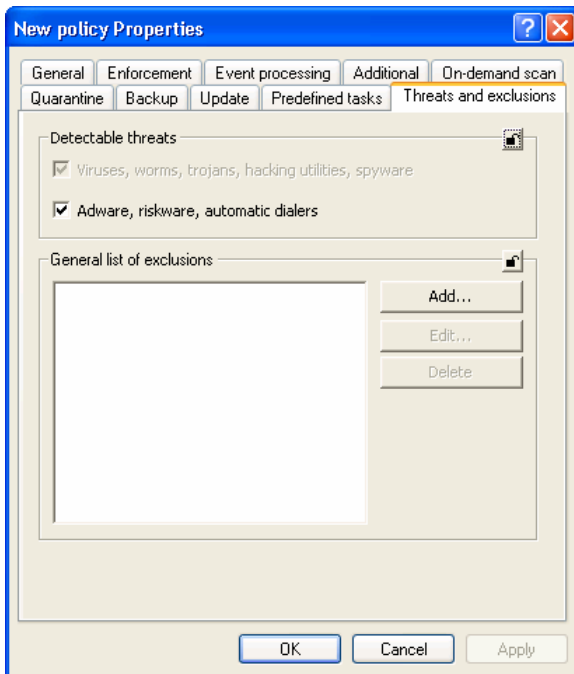
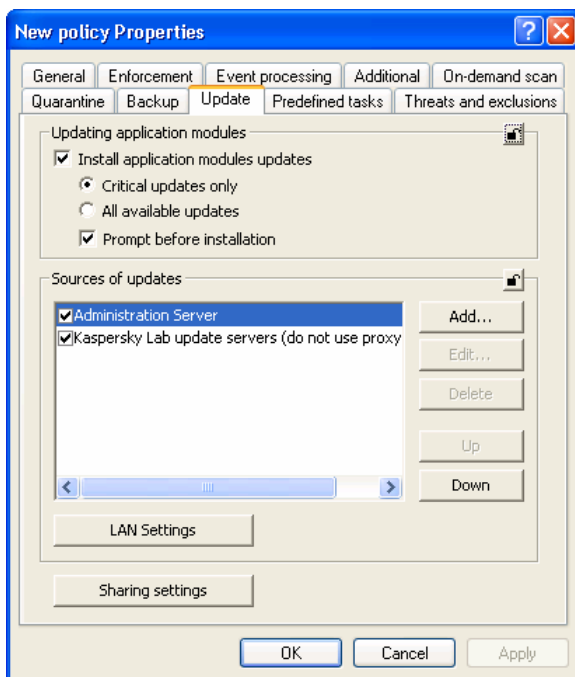


Figure 61. The **Threats and exclusions** tab

6.2.2.4. Updating anti-virus databases and application modules

On the **Update** tab (see Figure 62) you can customize the settings for updating the anti-virus database and application modules specified during creation of a new policy.

Figure 62. The **Update** tab

The **Update** tab consists of the following areas: **Updating application modules** – it is used for selection of parameters for the service updating the anti-virus databases and the application (see Step 4 on page 97). **Sources of updates** means the source of updates of the anti-virus database and application modules and its settings (see Step 3 on page 96).

Using the **LAN Settings** button you can configure the proxy server settings (details see section 5.1.3.4 on page 41). In the **Connection time-out (sec.)** field in the window that will open you can establish the timeout for establishing connection with the updates server (in seconds). When the specified time period elapses, the task will switch to the next updates sources in the list or will be aborted if no other updates sources are specified.

The window displayed after clicking the **Sharing settings** button lets the user enable copying of updates to a local resource and set up the copying settings (see section 5.1.3 on page 34).

6.2.2.5. Working with system tasks

In **Predefined tasks** tab (see Figure 63) you can enable/disable launching of scheduled system tasks.

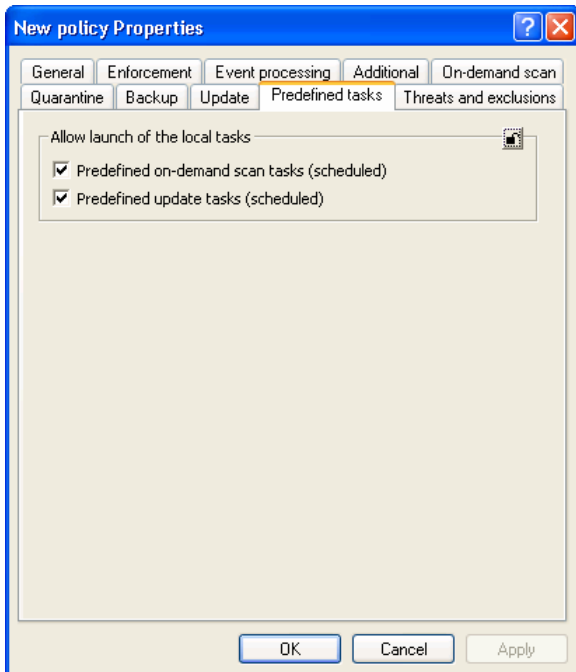


Figure 63. The **Predefined tasks** tab

6.2.2.6. Setting up Quarantine and Backup storage

The **Quarantine** (see Figure 64) and **Backup** tabs (see Figure 65) are used to specify the policy parameters for Quarantine and Backup storage.

These settings are identical to similar options for the Quarantine and Backup storage managed through a local interface (see section 5.8.1.1 on page 73).

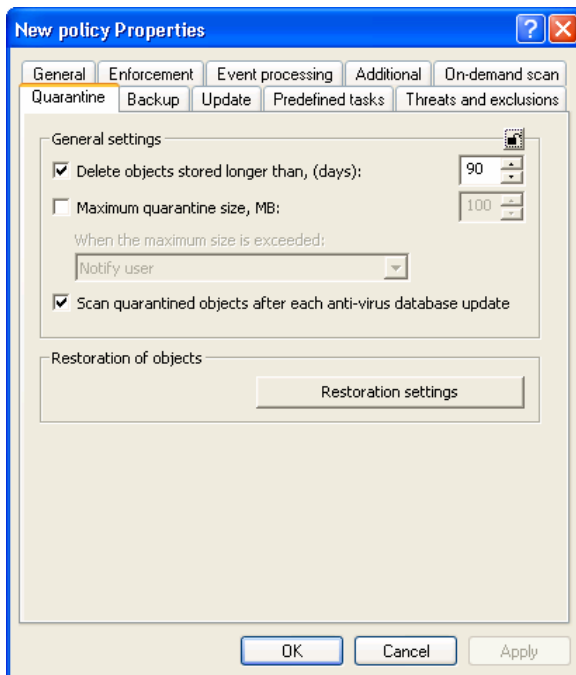


Figure 64. The **Quarantine** tab

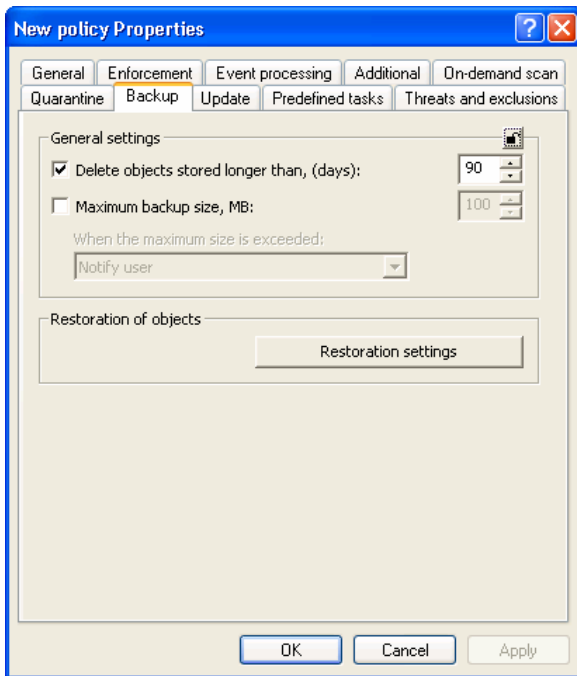


Figure 65. The **Backup** tab

6.2.2.7. Producing report on the operation of application

The **Event processing** tab (see Figure 66) displays the type of events occurring during the operation of application and registered in the report, as well as location of the report and conditions for notifying administrator and/or other users.

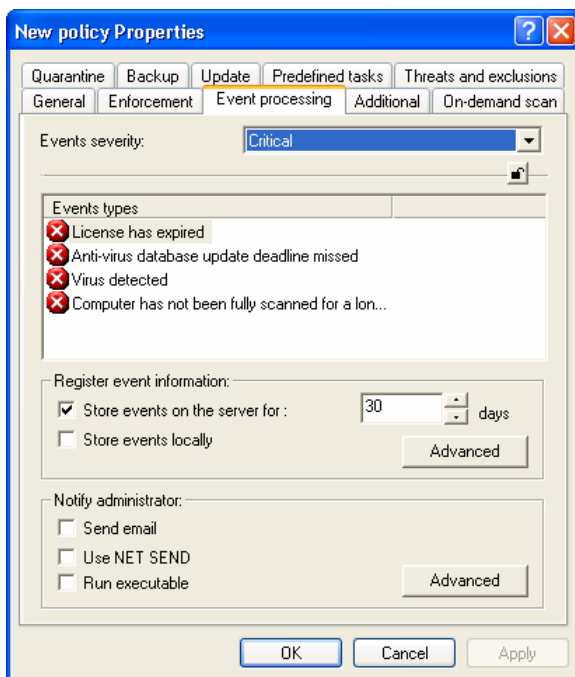


Figure 66. The **Event processing** tab

Kaspersky Anti-Virus SOS generates a set of events that occurred during the application operation. Each event has a priority status. There are four priority statuses:

- **Critical event;**
- **Error;**
- **Warning;**
- **Informational message.**

Events of the same type can be assigned different priority statuses, depending on the particular situation.

Select the event priority from the **Events severity** drop-down list. The information field below displays the event types for the selected priority level.

Table 2. Application events

Event	Level of importance
Object disinfected	Warning
Infected object deleted	Warning
Your license expires soon (two weeks before the expiration date)	Warning
Your license has expired	Critical event
License has not passed verification	Error
A suspicious object has been detected	Warning
Operation error	Warning Error
Anti-virus databases update deadline missed: – one week delay (couldn't find) – two weeks delay (couldn't find)	Warning Critical event
Virus detected	Critical event
Internal error	Error
Your operating system was restarted	Warning
The application was restarted	Warning
A password-protected archive detected	Warning
Object could not be disinfected	Warning
Your computer has not been fully scanned for a long time:	

Event	Level of importance
– for two weeks – for a month	Warning Critical event
Infected object blocked	Warning
Infected object skipped	Warning

* These values are the default values. You can alter them in the **Notification** dialog box (see section 6.2.2.8 on page 111).

You can indicate whether or not you want to include each event in the report as well as define administrator notification settings at the time of event occurrence.

For more detailed description of the **Event processing** tab refer to the Administrator's Guide for Kaspersky Administration Kit 5.0.

6.2.2.8. Additional parameters

The **Additional** tab (see Figure 67) displays the service settings of Kaspersky Anti-Virus 5.0 SOS. The majority of these settings are identical to the additional parameters described in section 5.8.4 on page 83.

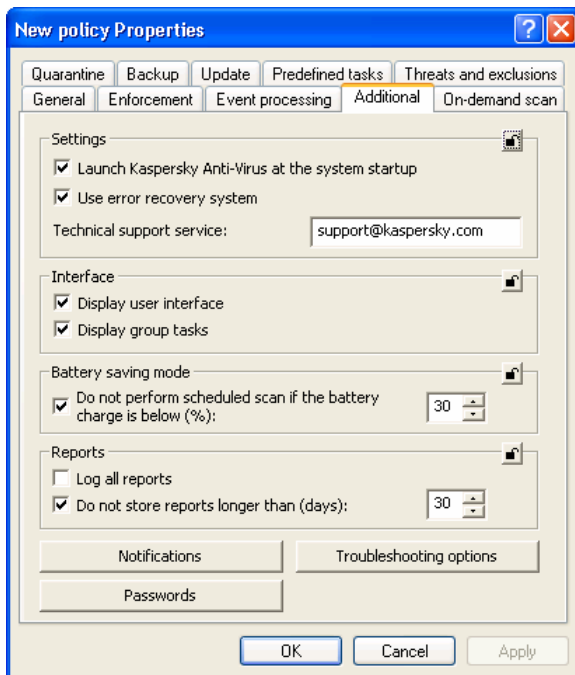


Figure 67. The **Additional** tab

You can set up the following passwords in the window that opens by clicking the **Passwords** button (see Figure 68):

- password for switching between the administrator's and the user's mode (see section 5.8.7 on page 89). In order to enable this mode, check the **Use password for application protection** box;
- password the user will be prompted for when attempting to uninstall Kaspersky Anti-Virus. This will help prevent any unauthorized attempt to uninstall Kaspersky Anti-Virus from the workstation.



Figure 68. The Passwords window.

In the window that appears when you click the **Notifications** button (see Figure 69), you can set the conditions for receiving various notifications:

- Display notifications when a dangerous object is detected** – enables display of messages informing the user that a virus has been detected.
- Display information messages** – disables display of Kaspersky Anti-Virus messages.
- Use system tray icon animation** – enable animation of Kaspersky Anti-Virus icon in the system panel during anti-virus scanning.
- Enable sound notification** – enable sound for the notifications appearing on the screen during the operation of Kaspersky Anti-Virus.

In **Event notifications** section you can define the settings for receiving notifications on the status of anti-virus database update and complete scanning of the computer. There are two levels for each of these tasks - a **warning** and a **critical event**.

For each event, in the field to the right you can set the number of days after expiration of which the user will receive daily corresponding notification when Kaspersky Anti-Virus is launched. This period of time will begin on the date of the last run of the corresponding task.

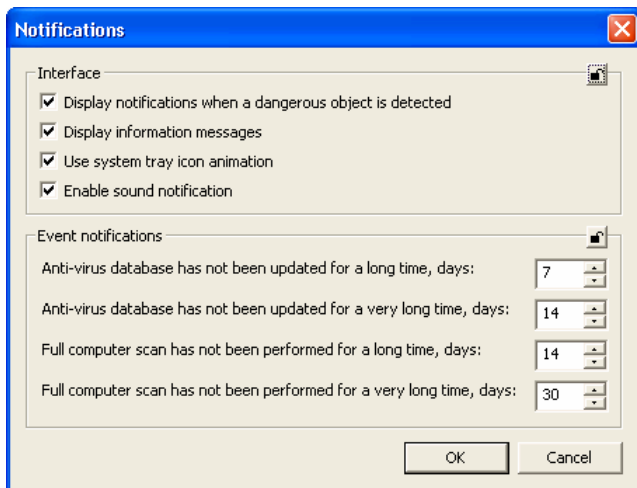


Figure 69. The **Notifications** window

Use the window (see Figure 70) that opens after clicking the **Troubleshooting options** button (see Figure 67) to configure the parameters optimizing the performance of on-demand scan tasks. You can:

- Disable scanning of e-mail accounts while running the task** – disable mail scanning while My Computer scan task is in progress
- Pause anti-virus scan when the system load exceeds (%)** – pause the anti-virus scan if the file system load is above the specified level. Specify the allowable system load level using a slider or the entry field to the right of the setting.

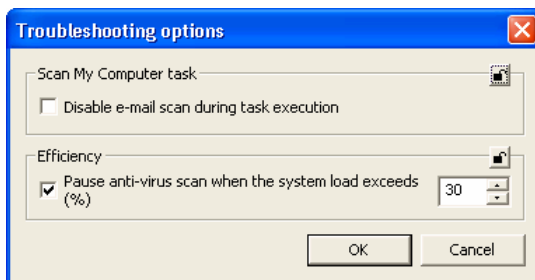


Figure 70. The **Troubleshooting options** window

6.2.2.9. Viewing results of policy application

The **Enforcement** tab (see Figure 71) displays the following information about the policy applied to the computers in this group:

- The number of computers this policy has been assigned to;
- The number of computers for which this policy has been enforced;
- The number of computers for which this policy is pending;
- The number of computers for which this policy has failed.

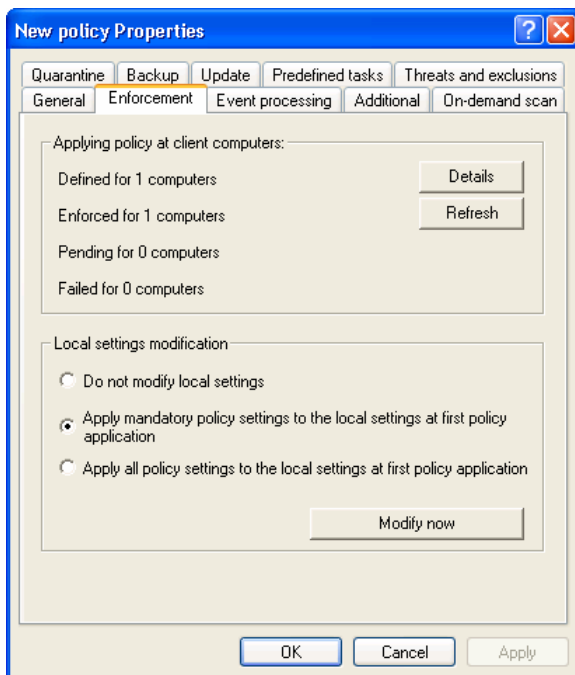




Figure 71. The **Enforcement** tab

Click **Details** to open a dialog box containing details about the selected policy applied to each client computer. (details, see the Reference Guide for Kaspersky Administration Kit 5.0.)

In **Local settings modification** section you can specify which of the settings will be changed in the policies of nested groups, in the application's and tasks' settings on the client computers the first time the policy is applied. You can select one of the following options:

- **Do not modify local settings.** In this case the local settings will not be changed.
- **Apply mandatory policy settings to the local settings at first policy application.** In this case only local settings marked with the  icon will change. In order to prevent such user from changing the required settings on the client computer, left click this icon. It will change to .
- **Apply all policy settings to the local settings at first policy application.** In this case, all local settings will change according to the policy settings. As with the previous options, you can prevent user from changing the required settings.

The local settings will change automatically the first time you apply policy on the client computer. If you would like to reapply the policy with modified settings, press the **Change now** button.

6.3. Managing tasks

This section describes how to create and manage tasks for Kaspersky Anti-Virus 5.0 SOS. Detailed information about managing tasks see the Administrator's Guide for Kaspersky Administration Kit 5.0.

6.3.1. Creating a task

During application setup a list of system tasks is generated for each computer. The list (see Figure 72) includes on-demand scanning tasks (scanning My Computer, automatic scanning at the launch of Kaspersky Anti-Virus, scanning quarantine) and updating tasks (updates of the anti-virus databases, updates of application modules, roll-back feature for the updates to anti-virus databases).

A schedule is provided for on-demand scanning tasks and updating anti-virus databases.



You can start the system tasks and edit their parameters and schedule, but these tasks cannot be deleted.

Using Kaspersky Administration Kit, you can create the following tasks for Kaspersky Anti-Virus:

- Local tasks assigned to each client computer;
- Group tasks assigned to the groups of client computers;

- Global tasks assigned to a set of client computers from arbitrary groups on a logical network.

You can change task settings, control their execution, copy and remove tasks from one group to another, and delete them using the standard shortcut menu commands, such as **Copy/Paste**, **Cut/Paste**, and **Delete**, or similar commands in the **Action** menu.

The application parameters for each client computer while executing tasks comply with the group policy, specific task settings, and the application settings on this client computer.

All tasks are scheduled by default. Tasks can be temporarily excluded from the list of scheduled tasks. In this case, the tasks are not deleted from the task list; they are simply not launched.

You can manually launch, abort, stop, or resume a task using the commands **Start/Stop/Pause/Resume** in the shortcut menu or in the **Action** menu.

6.3.1.1. Creating a local task



To create a local task, you should perform the following actions:

1. In the **Groups** folder, select a folder with the name of the group that includes the required client computer.
2. On the results pane, select the computer the new local task will be applied to and click the **Properties** command in the shortcut menu or in the **Action** menu. You will see the **<Computer name> Properties** dialog box with the properties of the client computer (see Figure 72).
3. Open the **Tasks** tab (see Figure 72). It shows a complete list of scheduled tasks for this client computer.
To create a new local task, click **Add**. Click **Properties** to change the task settings and **Delete** to delete the selected task.

Click **Add** to create a new task. The interface of the application for creating a new task is organized as a Microsoft Windows wizard, which will guide you through the process. To switch between the wizard dialog boxes, click **Back** and **Next**. To finish working with the wizard, click **Finish**. To stop working with the wizard at any stage, click **Cancel**.

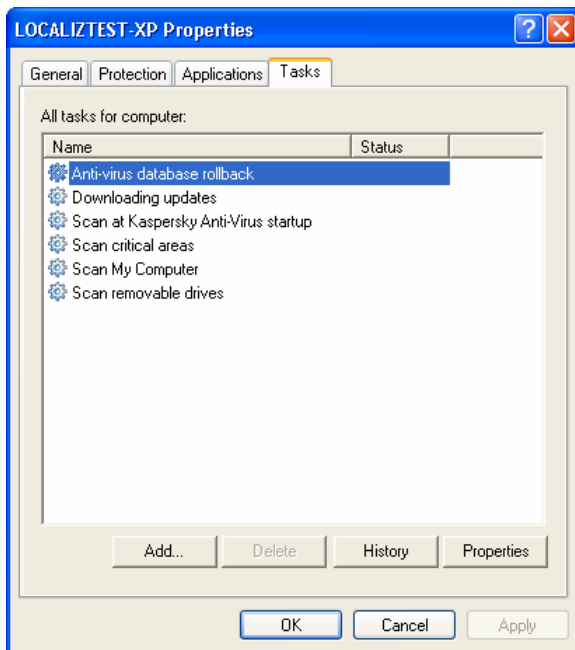


Figure 72. Creating a local task
The **Tasks** tab

Step 1. General information about the new task

The first wizard dialog box is introductory: here you should enter the task name (**Name** field).

Step 2. Select the application and type of the task

Select **Kaspersky Anti-Virus 5.0 SOS**. application from the **Choose the application for which to define a task** drop-down list. Then pick up the type of the task from the **Choose type of task for execution** drop-down list. The following tasks can be created for Kaspersky Anti-Virus SOS:

- **Update anti-virus databases and application modules** – Updates the anti-virus databases and application components.
- **Anti-virus databases rollback** – Rolls back anti-virus database updates;
- **On-demand scan** – scans objects on-demand;
- **Install license key** – Installs license keys;

Step 3. Configure settings for the selected task type

Depending on the selected type of the task, you will be given several options on how to configure the following task settings:

ANTI-VIRUS DATABASE AND APPLICATION MODULES UPDATE TASK SETTINGS

The task settings for updating the anti-virus databases and application modules are configured similarly to the case of creating a new policy (see Step 3– Step 4 on pages 96–97). In addition, during task creation you may define, for example, the parameters for sharing updates received (see section 5.1.3.2 on page 38).

CONFIGURE ANTI-VIRUS DATABASE ROLLBACK TASK SETTINGS

The task for rolling back the updates of the anti-virus databases has no specific settings. Therefore, after you select this task, the wizard will bring you to the **Task scheduling settings** dialog box (see section 5.6 on page 68)

ON-DEMAND SCANNING TASK SETTINGS

Select the anti-virus protection level for the on-demand scanning task (see section 4.2 on page 29) and specify action to be performed with the detected malicious object (see section 5.2.3.2 on page 54).

Clicking the **Advanced** button opens a window where you can review the settings for the selected anti-virus protection level or use them as the basis for custom adjustments. That will change the level of protection to **Customized**.

In the next dialog box (see Figure 73), specify the objects to be scanned using **Add**, **Edit** and **Delete** buttons.

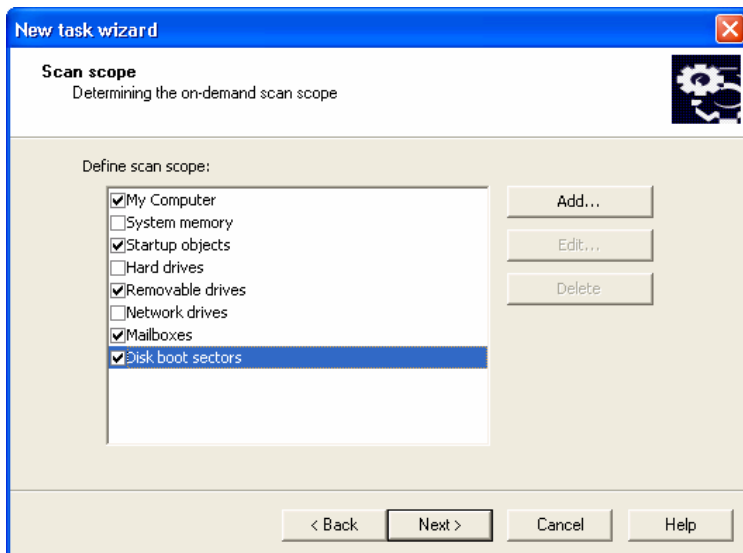


Figure 73. List of objects to be scanned

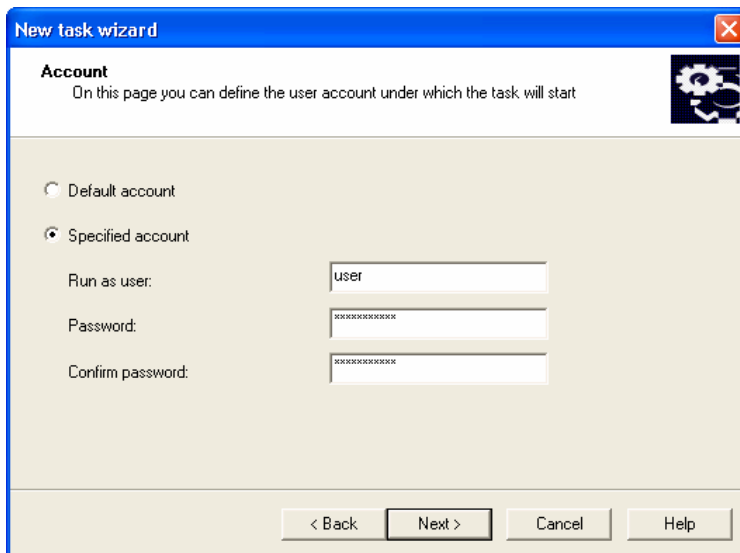
INSTALL LICENSE KEY TASK SETTINGS

Use the **Browse** button to locate the path of the key file. To make the key being added your current key, check the box **Use as the current license key**.

Do not check this box if the key is added as a reserve key. An additional license key becomes your current key when the current license key expires.

Step 4. Configuring tasks launching under a selected user's account

During this step (see Figure 74) you can configure the launch of the task being created under a user's account that has sufficient access rights to the object to be scanned or to the update source (details see para 5.7 on page 71).



The screenshot shows a 'New task wizard' dialog box with a blue title bar and a close button in the top right corner. The main area is titled 'Account' and contains the instruction: 'On this page you can define the user account under which the task will start'. There is a gear icon in the top right of the main area. Below the instruction, there are two radio buttons: 'Default account' (unselected) and 'Specified account' (selected). Under 'Specified account', there are three input fields: 'Run as user:' with the text 'user', 'Password:' with masked characters 'XXXXXXXXXX', and 'Confirm password:' with masked characters 'XXXXXXXXXX'. At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Figure 74. Configuring running a task under a different user's account

Step 5. Configure a schedule

After you have configured the selected task, the wizard will open the **Task scheduling settings** dialog box (see Figure 75), where you can schedule this task.

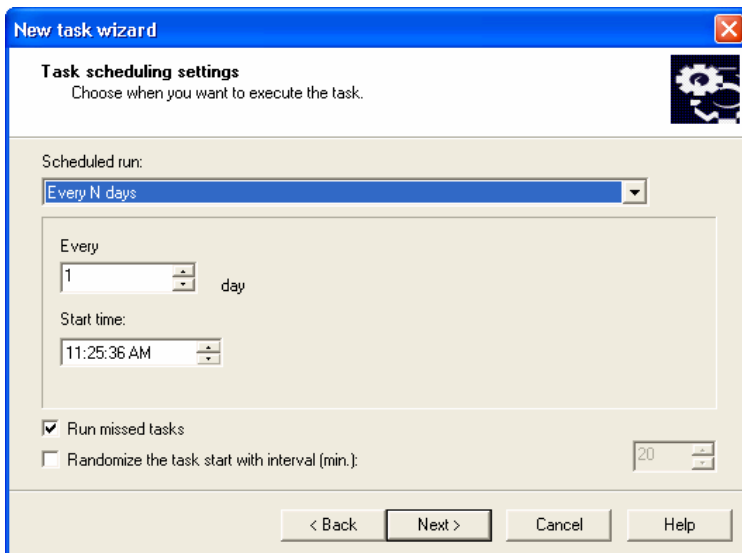


Figure 75. Configuring schedule during a new task creation

Select the desired regularity for the task from the **Scheduled run** drop-down list. The following options will be available: *Every N hours*, *Every N days*, *Every N weeks*, *Manually* and *At application start*. Depending on your choice, the elements of this dialog box will vary:



Tasks for anti-virus database update rollback and license key installation can only be launched manually.

Please see details on scheduling automatic task launch in the Administrator's Guide for Kaspersky Administration Kit 5.0.

Step 6. Completing task creation

The last wizard dialog box will inform you that the task has been successfully created.

6.3.1.2. Creating a group task



To create a group task for Kaspersky Anti-Virus, you should perform the following actions:

1. In the console tree, select the group of computers the new task will be applied to.
2. Select the **Group tasks** folder within this group, open the shortcut menu, and select the **New/Task** command. You can also select this command in the **Action** menu. A wizard for creating a new group task that will guide you through the creation process will appear. The wizard is organized similarly to the local task wizard (see section 6.3.1.1 on page 117).

After the task is created, it will be added to the **Group tasks** folder for the selected group and all nested groups and displayed on the results panel.

6.3.1.3. Creating a global task



To create a global task for Kaspersky Anti-Virus, you should perform the following actions:

1. In the console tree, select the **Global tasks** node, open the shortcut menu, and select the **New→Task** command. You can also select this command in the **Action** menu.
2. A wizard for creating a new global task that will guide you through the creation procedure will appear. The wizard is organized similarly to the local task wizard (see section 6.3.1.1 on page 117 about the local task wizard). The only difference is that you should define a list of client computers on the logical network for this global task.
3. Select the desired computers on the logical network that the new task will be assigned to. You can either select computers from different folders or select the entire folder (for more details, see the Reference Guide for Kaspersky Administration Kit 5.0).



Global tasks are applied only to the specified set of computers. For example, the remote installation task assigned to a group will not be performed on new client computers added to this group. You will have to create a new task or make appropriate changes to the existing task.

After the task is created, it will be added to the **Global Tasks** node of the console tree and displayed on the results panel.

6.3.2. Viewing and editing task settings and monitoring task performance



To view and / or edit task settings:

- For a local task, in the **Groups** folder, select the folder with the name of the group that includes the client computer. On the results panel, choose the required computer and click **Properties** in the shortcut menu. This will open the **Properties: <Computer Name>** dialog box. In this dialog box, switch to the **Tasks** tab (see Figure 72). You can view and edit selected task settings in the window, which will appear when you click on the **Properties** button.



The **Tasks** tab displays a full list of tasks assigned to this local computer, including both global and group tasks. Global and group tasks are marked with a “folder” icon. Note that you can view settings for all tasks but edit only those for local tasks.

- For a group task, select the required group in the console tree and choose the **Group tasks** folder within this group. The results panel will display all tasks assigned to this group. Select the desired task, open the shortcut menu, and click **Properties** (or click **Properties** in the **Action** menu).
- To modify global task settings, select the **Global tasks** node in the console tree, choose the desired task, open the shortcut menu, and click **Properties** (or click **Properties** in the **Action** menu).

You will see the **Properties: Task name** dialog box, consisting of the following tabs: **General**, **Settings**, **Account**, **Schedule**, and **Notification**. The global task configuration dialog box contains an additional tab **Target computers** for which the task will be created.

All tabs (except for the **Settings** and the **Account** tab) are standard tabs for Kaspersky Administration Kit 5.0. Details about these tabs are available in the Kaspersky Administration Kit Administrator's Guide. The **Settings** tab displays specific settings for Kaspersky Anti-Virus SOS, depending on the selected task's type (see Step 3 on page 119). The **Account** tab is used to configure launching of the tasks on behalf of the account (see section 5.7 on page 71).

6.3.3. Launching and stopping tasks



The tasks on the computer can be started only if the corresponding application is running. When the application is terminated, all running tasks are also aborted.

All tasks can be launched and stopped either automatically, according to the schedule, or manually, using the shortcut menu options or from the settings viewing window. You can also pause a running task and then resume it.



To start / stop / suspend / resume a task manually:

select the required task, open the shortcut menu, and select the **Start / Stop/ Suspend/ Resume** command in the shortcut menu or in the **Action** menu.

Similar commands can be accessed from the task configuration window on the **General** tab corresponding buttons (see section 6.3.2 on page 124).

6.4. Configuring application settings

You can change application parameters for individual client computers in a group. You can redefine only those settings that are defined as modifiable by the policy for the application.



To change application settings:

1. In the **Groups** folder, select the folder with the name of the group that includes the client computer.
2. On the results panel, select the computer for which you want to change application settings and click the **Properties** command in the shortcut menu or in the **Action** menu.
3. As a result, the **Properties: <Computer name>** dialog box, consisting of the four tabs, will be displayed in the program main window. Select the **Applications** tab (see Figure 76) that displays a full list of Kaspersky Lab applications installed on that client computer.
4. Select **Kaspersky Anti-Virus 5.0 SOS**. Below the list, you can see the **Events**, **Statistics**, and **Properties** buttons that serve to:

- View a list of events occurred on the client computer and logged on the administration server (for report details, see the Reference Guide for Kaspersky Administration Kit 5.0).
- View current statistics about application performance.
- Access application settings. Clicking the button opens a window including the following tabs: **General**, **Additional**, **Threats and Exclusions**, **Potentially Dangerous Programs**, **Quarantine**, **Backup**, **Storage objects**, **Licenses**, and **Event processing**. Please see detailed description of these tabs below.

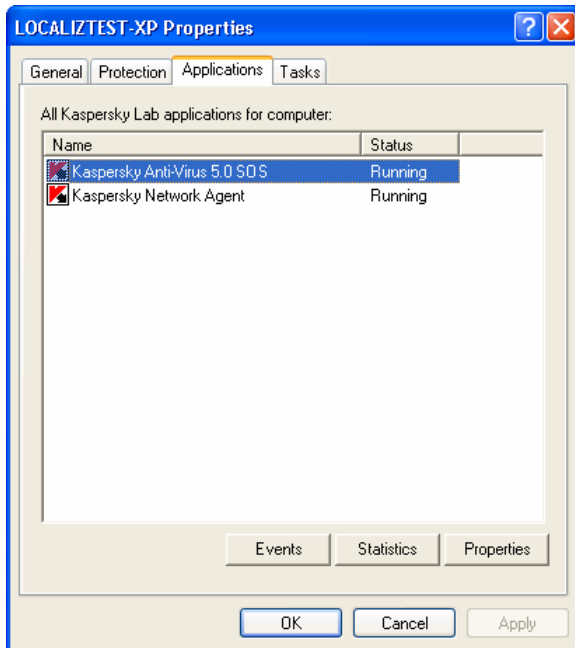


Figure 76. Client computer properties dialog box
The **Applications** tab

6.4.1. Viewing information about the application

In the **General** tab (see Figure 77) you can examine general information about the application (Kaspersky Anti-Virus 5.0 SOS); start or stop its operation.

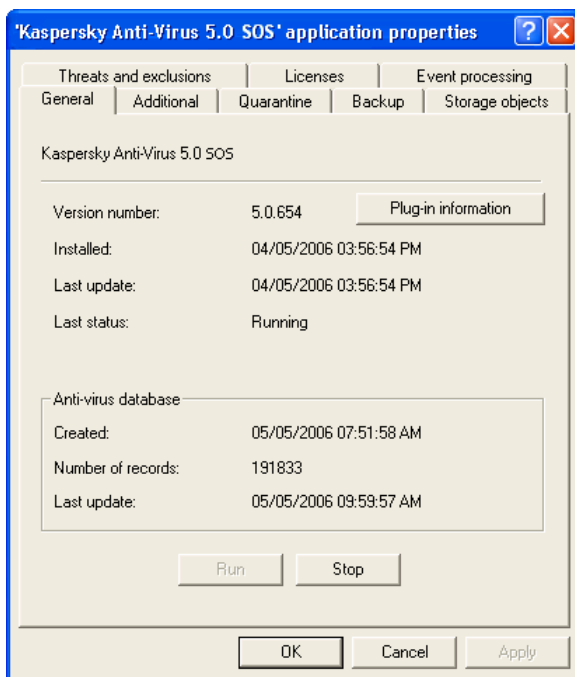


Figure 77. Application setup window. The **General** tab

The upper portion of the window displays the title of the installed application, its version, date of installation, its status (whether the application is running or stopped on a local computer) as well as the information about the condition of the anti-virus databases.

You can start / stop application activity using the corresponding buttons.

Using the **Plug-in information** button you can view general information about the Kaspersky Anti-Virus 5.0 SOS administration plug-in (see Figure 78)

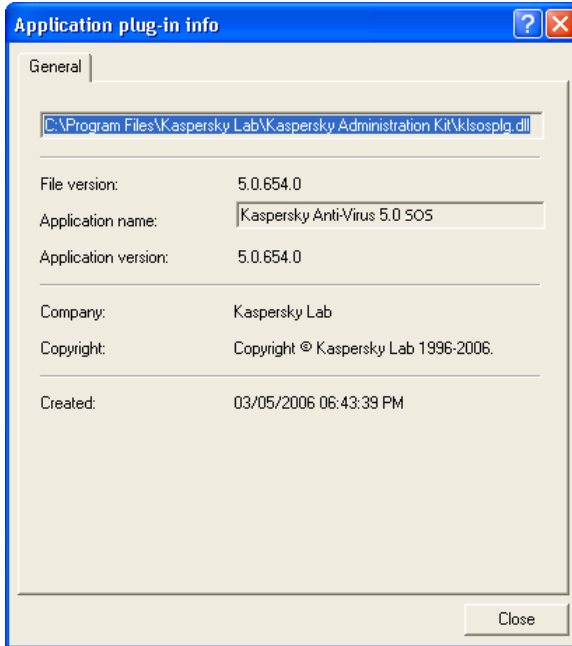


Figure 78. Information about the application administration plug-in

6.4.2. Additional application settings

The **Additional**, **Quarantine**, **Threats and exclusions**, and **Backup** tabs are used for setting the parameters of Kaspersky Anti-Virus SOS on a remote workstation.

These application settings duplicate the corresponding group policy settings (see details in section 6.2.2 on page 99). The policy settings remain predominant for application setup.



When configuring application settings on a local computer, you can change only the parameters that the group policy allows to be modified.

6.4.3. Working with the quarantine and backup storage areas

Kaspersky Anti-Virus 5.0 SOS stores suspicious objects and backup files in special storages.

Each computer has its own quarantine and backup storage directories.

You can review objects quarantined and backed-up on a computer using the **Storage objects** tab (see Figure 79).

To do so click the **List of objects** button in the **Quarantine** or **Backup storage** section respectively.



If the application cannot establish a connection to the client computer, a dialog box will be displayed with a choice of retrying or canceling connection attempts.

The dialog boxes displaying the contents of both storage areas are similar (see Figure 80). In the central part of the dialog box, you can see a list of quarantined or backup files. The following information is available for each object: name, status, date of its relocation to quarantine and original path to the object.

Above the list, there is a toolbar for managing quarantined objects or backup copies. Use the following buttons to:



– Restore an object. Click this button to restore the object, specifying the location in which it will be restored.



In the event of remote management by Kaspersky Administration Kit objects can be restored only to a computer, where *Administration Console* is installed.



– Delete the object from the storage folder.



– Refresh the storage contents.



– Scan objects (for Quarantine only).

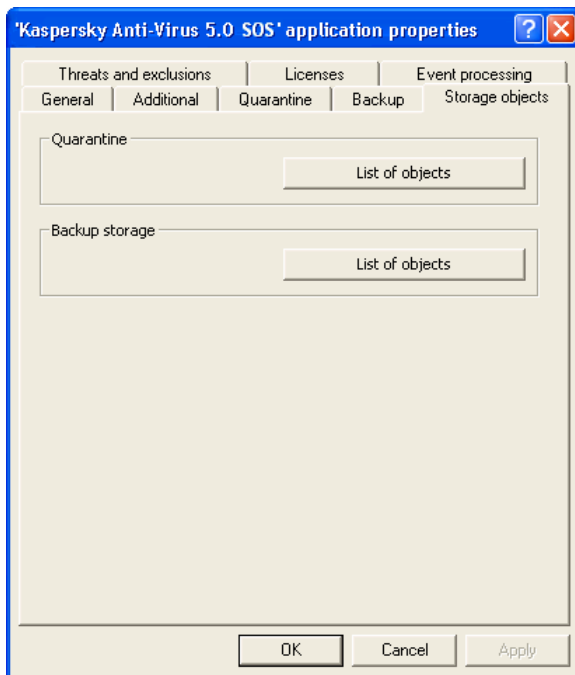
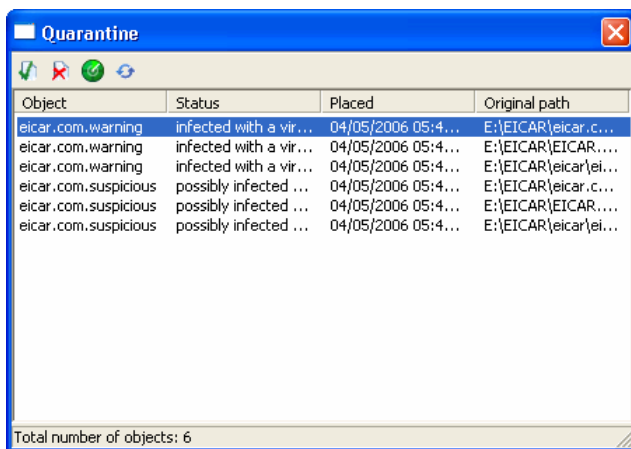
Figure 79. The **Storage objects** tab

Figure 80. Quarantine storage

6.4.4. Viewing information on license keys

The **Licenses** tab (see Figure 81) is purely informational. It displays information about the current and the reserve license keys installed on a specific computer.

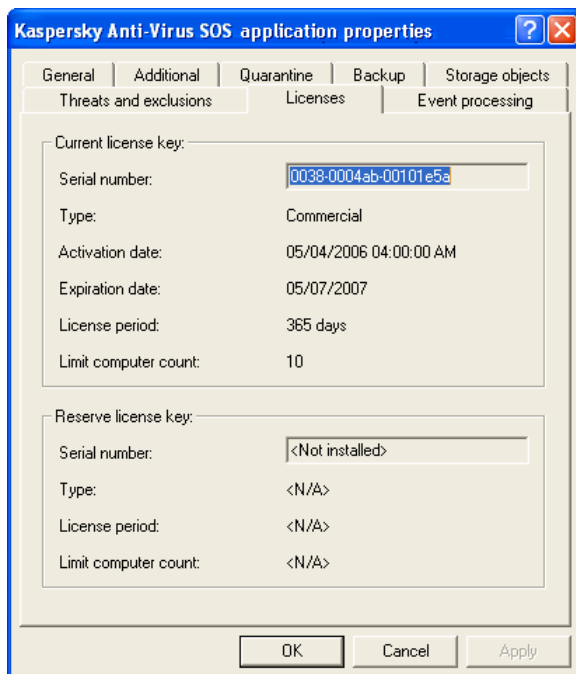


Figure 81. The **Licenses** tab

6.4.5. Setting up report generation parameters


The **Event processing** tab provides access to the parameters for the messaging service, which sends notifications about Anti-Virus operation from a remote computer.

This tab duplicates the parameters of the corresponding group policy tab (see section 6.2.2.7 on page 108).

CHAPTER 7. TESTING OPERATION OF KASPERSKY ANTI-VIRUS

7.1. Test “virus” EICAR and its modifications

After installing and adjusting Kaspersky Anti-Virus, we recommend that you test the correctness of its settings and operation of the application using a test “virus” or its modifications.

The test virus was specially designed by the  organization (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test “virus” IS NOT ACTUALLY A VIRUS because it does not contain code that can really 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 the test “virus” from the official website of the **EICAR** organization at http://www.eicar.org/anti_virus_test_file.htm.

The file downloaded from the **EICAR** website or created as described above contains the body of a standard test “virus.” Kaspersky Anti-virus application will detect it, assign it to the **Infected** category, and apply the action defined by the administrator for handling objects belonging to that type.

To test the response of your anti-virus application to other types of objects, modify the body of this standard test “virus” by adding one of the prefixes listed in Table 3.



You can test the correctness of Kaspersky Anti-Virus operation using the modified EICAR “virus” only if your anti-virus database was last updated on or after October 24, 2003, or has the cumulative updates for October, 2003.

Table 3. Test “virus” modifications

Prefix	Object type
No prefix, standard test “virus”	Infected – An error occurs during an attempt to cure an object; the object gets deleted.
CORR–	Corrupted
SUSP–	Suspicious (unknown viral code)
WARN–	Warning (modified code of a known virus)
ERRO–	Error when scanning the object
CURE–	Infected – The object is disinfected; the text of the “virus” body is changed for CURE
DELE–	Infected – The object is automatically deleted

The first table column lists prefixes to be added at the beginning of the string of the standard test “virus”.

After adding a prefix to the test “virus” save it, for example, to a file under the name eicar_dele.com; assign names to all the modified “viruses” in the same manner.

The second column of this table contains the types of objects identified by an anti-virus application after you have added a prefix. The actions for each type of objects are defined by Kaspersky Anti-Virus application settings customized by the administrator.

7.2. Testing correct operation of Kaspersky Anti-Virus



In order to test the correctness of settings and performance of Kaspersky Anti-Virus 5.0 SOS:

- Make a directory on disk and save the test “viruses” which you have created to it.

- Create a custom user task and define its parameters (see section 5.4 on page 63):
 - add the folder containing created test “viruses” to the list of objects scanned when the task is run;
 - select the *Prompt user for action during the scan* option as the action to be performed by Kaspersky Anti-Virus when it detects infected or suspicious objects.
- In the **Additional settings** dialog box (see section 5.8.4 on page 83) check the box **Log all reports** to save data about corrupted objects or objects which could not be checked because of errors.
- Run the task.

During the scanning procedure, as soon as suspicious or infected objects are discovered, the application will display a dialog box containing information about any such object and ask the user to select the appropriate action. E.g., if an object with the SUSP- prefix is detected, you will see the following message:



Figure 82. Attention! A suspicious object detected

Thus you can test reaction of Kaspersky Anti-Virus to discovering objects of different types by selecting various options in the dialog boxes displayed during scanning.

Complete summary of scanning results will appear in the report (see Figure 83).

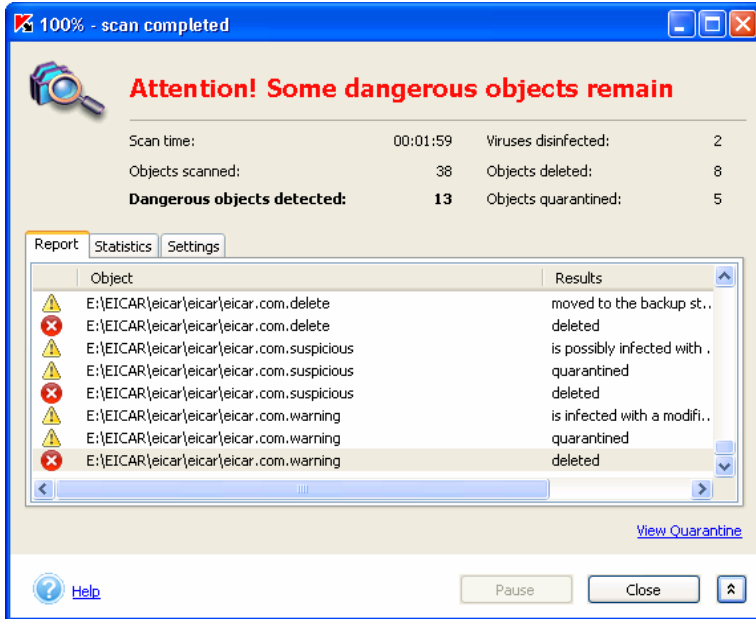


Figure 83. The report on scanning the directory containing test "viruses"

CHAPTER 8. MANAGING LICENSE KEYS

You can use Kaspersky Anti-Virus only after you install the license key included into the product installation kit.



Kaspersky Anti-Virus SOS DOES NOT work without a license key!

When the license expires, the functionality of Kaspersky Anti-Virus remains unchanged except that you will not be able to update your anti-virus database. You will still be able to scan your computer and e-mail and disinfect dangerous objects, but you'll be using old anti-virus databases valid by the date when your license expired. Therefore, we do not guarantee complete protection from new viruses which may appear after expiry of your Kaspersky Anti-Virus license.

In order to avoid the infection of your computer with new viruses, we recommend that you renew your Kaspersky Anti-Virus license.

Two weeks prior to expiry of the license Kaspersky Anti-Virus will display notifications. For two weeks you will see a warning message every time at the application startup.



In order to renew your license, you will need to purchase and install a new license key for Kaspersky Anti-Virus. In order to do so:

1. Contact the company you purchased the product from and acquire a new license key for using Kaspersky Anti-Virus 5.0 SOS;

or:

purchase the license key directly from Kaspersky Lab by following the [Renew license](#) link on the **Support** tab (see Figure 4) or by pressing the **Renew** button in the **Managing License Keys** window (see Figure 84). Fill out the form at our website page that will open. Upon your payment you will receive a link at the e-mail address you specified in the order form. Follow this link to download the license key.



Kaspersky Lab periodically announces campaigns that allow you to enjoy considerable discounts when you renew your license for the use of our products. In order to keep informed about our offers visit Kaspersky Lab's corporate website and go to **Products → **Sales and special offers**.**

2. Install the license key file. Please see details on work with the license key using a local license key interface in section 8.1 on page 137; for

details pertaining to the use of the Kaspersky Administration Kit interface, please see section 8.2 on page 140.



You can install two keys: a current key and a backup key. The current key is the key that is currently in use by the application. The application can not have more than one key with the “current” status. The backup key will be activated as soon as the current key expires.

8.1. Managing keys using local interface



In order to renew your license via a Kaspersky Anti-Virus SOS local interface:

1. Purchase a license key (details see above).
2. Install the license key. In order to do it:
 - a. Follow the [License Keys](#) link in the left section of the **Support** tab (see Figure 4).
 - b. In the **Managing License Keys** window (see Figure 84), press the **Add** button.
 - c. Using the standard file select dialog box, switch to the folder where the license key is located (file with **.key** extension). Select the key you need and press the **Open** button.
 - d. Read information about the key you are adding In the **License Key Activation** window that will open (see Figure 85) press the **Activate** button in order to start using this key.

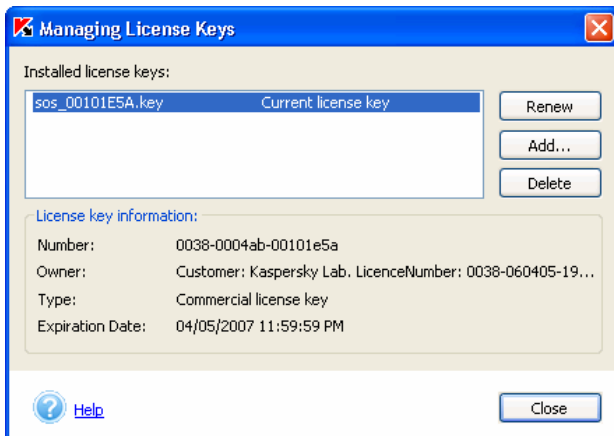


Figure 84. License key management window

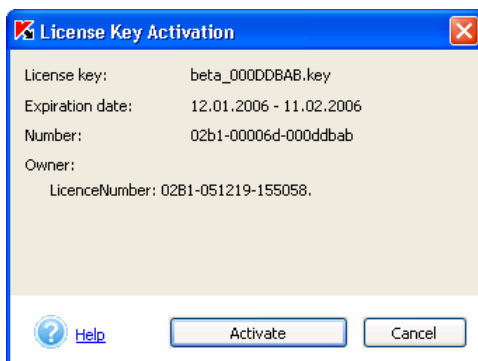


Figure 85. Key activation window

or.

- a. Select the Kaspersky Anti-Virus group in the **Start** → **Programs** menu and select the **Install License Key** item.
- b. Press the **Browse** button In the window that will open and select the folder in which the license key file is located.
- c. Select the required license key and press the **Open** button.
- d. In the bottom part of the dialog box (see Figure 86), check the box next to the name of the application for which the license key is to be installed. Press the **OK** button.



If the list in the bottom part of the dialog box is empty, this means the license key is not suitable for any of the Kaspersky Lab applications installed on your computer.

Select another license key file.

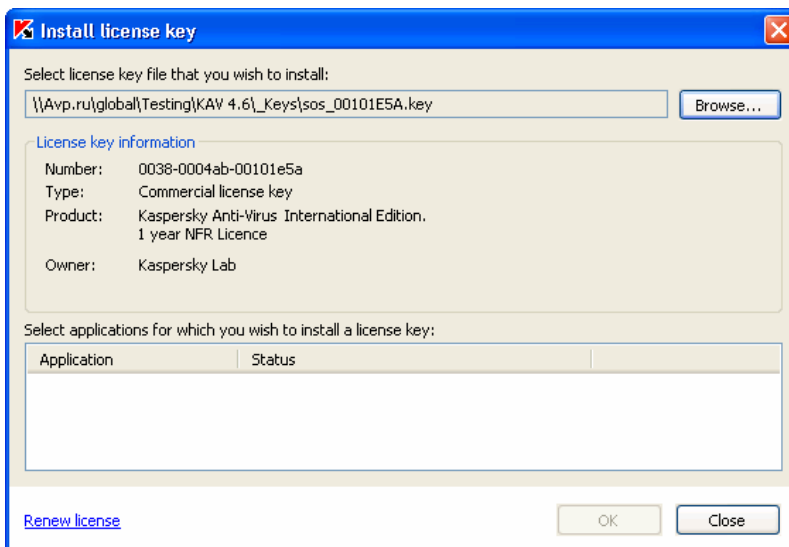


Figure 86. The **Install license key** dialog box.

- e. Review information about the key being added in the **License Key Activation** dialog box that will open (see Figure 85) and press the **Activate** button to start using the key.

If you are adding a new key while the current key is still valid, you will be offered to choose from two key installation options:

- You can make the key you are adding a backup key (recommended). If you select this option, the key will be added to the list with the *backup key* status. After the current key expires, this new key will be automatically assigned the *current* status.
- Replace the current key with the new key. If this option is selected, the new key will be added to the list with the *current* status.



Please note that if you delete the current key, the backup key you installed will also be deleted automatically!

8.2. Working with license keys using the Kaspersky Administration Kit interface

If the package is controlled via Kaspersky Administration Kit, you can extend a license using either of the following two methods:

- *Add group license* means extension of the license for Kaspersky Anti-Virus simultaneously for selected computers or groups of client computers using global or group tasks (details see in the Administrator's Guide for Kaspersky Administration Kit 5.0).
- *Add an individual license* means extension of the license for Kaspersky Anti-Virus for an individual computer.



In order to extend a workstation license you have to purchase and install a new license key for Kaspersky Anti-Virus. To do so:

1. Purchase a license key (see Chapter 8 on page 136).
2. Create a local task for license key installation (see section 6.3.1.1 on page 117).

You can review the information about the license keys (current and reserved) installed on a specific computer within the **Licenses** tab (see section 6.4.4 on page 131).

CHAPTER 9. MANAGING APPLICATION FROM THE COMMAND LINE

Kaspersky Anti-Virus can be managed from the command line using the **kavshell.exe** utility included into the distribution package. After Kaspersky Anti-Virus installation this utility is located in the application installation root folder. When you start this utility from the command line, depending on the commands used, the following functions will be available:

SCAN	Scan of selected objects
FULLSCAN	Full computer scan
UPDATE	Updating anti-virus database and application modules
ROLLBACK	Rollback of the last anti-virus database update
START	Starting Kaspersky Anti-Virus
STOP	Stopping Kaspersky Anti-Virus
TASK	Managing Kaspersky Anti-Virus tasks
IMPORT	Importing Kaspersky Anti-Virus settings from a file
EXPORT	Exporting Kaspersky Anti-Virus settings to a file
ADDKEY	Adding a license key



If the use of the user's and administrator's mode is disabled in the Kaspersky Anti-Virus settings (see section 5.8.7 on page 89), commands that require password will not be performed. In this case an error message will be displayed.

To view the command syntax use:

```
KAVSHELL HELP [command] 3
KAVSHELL [command] /?
```

If the **key** modifier is not specified, the list of all available commands will be displayed

Examples:

```
KAVSHELL HELP SCAN
KAVSHELL SCAN /?
```

9.1. Scanning selected objects

Command syntax:

```
KAVSHELL SCAN [objects] [/L[!]:objects_file] [/F(A|E|C)]
[/NP] [/ASK|/DISINFECT|/DELETE] [/W[A][!]:report_file]
```

If no modifiers are specified, command syntax help will be displayed.



Scan task will be performed with the settings recommended by Kaspersky Lab's experts.

Modifier	Purpose
objects	<p>Creates the list including one or several files, folders or pre-defined objects separated with a space:</p> <p>Types of pre-defined objects are as follows:</p> <ul style="list-style-type: none"> • /MEMORY – system memory; • /STARTUP – startup objects; • /MAIL –Microsoft Office Outlook

³ Optional keys are provided in square bracket.

	<p>and Microsoft Outlook Express mailboxes;</p> <ul style="list-style-type: none"> • /REMDRIVES – removable drives; • /FIXDRIVES – system drives; • /NETDRIVES – network drives. <p>Comments:</p> <ul style="list-style-type: none"> • if an object's name contains a space, it must be provided in double quotes; • if you wish to scan several files, you can use masks (masks examples see section 5.5 on page 64); • if a specific folder is specified, all files contained in it will be scanned.
/L[!]:objects_file	<p>Creates a file in .txt format that contains the list of objects to be scanned (files, folders, pre-defined objects). Name of each object in the file must start from a new line. The ! symbol is used for deletion of the objects file after the scan is completed.</p> <p>You can use either absolute or relative path to the file. If the path contains spaces it must be provided in double quotes.</p>
/F(A E C) /FA /FC /FE	<p>Types of files to be scanned:</p> <ul style="list-style-type: none"> • scan all files. • scan all infectable files based on their formats. • scan all infectable files based on their extensions.
/NP	Skip password-protected objects
[/ASK /DISINFECT /DELETE] /ASK /DISINFECT	<p>Actions to be performed with an infected object:</p> <ul style="list-style-type: none"> • Prompt user for action. • Disinfect, delete if disinfection is not

/DELETE	<p>possible.</p> <ul style="list-style-type: none"> • Delete. <p>Comments:</p> <ul style="list-style-type: none"> • if no action is selected, the object will be skipped and information about its detection will be logged in the report • composite files will not be deleted.
/W[A][!]:report_file /W: report_file /WA: report_file	<p>Logging events into the specified report_file:</p> <ul style="list-style-type: none"> • only important events; • all events. <p>Symbol ! is used to force the report file to overwritten each time the task is started.</p> <p>You can use either absolute or relative path to the file. If the path contains spaces it must be provided in double quotes.</p>

Example:

```
KAVSHELL SCAN "C:\Program Files" C:\Downloads\test.exe
/MEMORY /STARTUP /FA /DISINFECT /WA:log.txt
KAVSHELL SCAN /MEMORY /STARTUP C:\Downloads\test.exe /FC
/W:log.txt /ASK
```

9.2. Full scan

Command syntax:

```
KAVSHELL FULLSCAN [/W[A][!]:report_file] [/D]
```

If no modifiers are specified, command syntax help will be displayed.



Scan task will be performed with the settings recommended by Kaspersky Lab's experts.

Modifier	Purpose
/W[A][!]:report_file /W:report_file /WA:report_file	Logging events into the specified report_file: <ul style="list-style-type: none"> • only important events; • all events. Symbol ! is used to force the report file to overwritten each time the task is started. You can use either absolute or relative path to the file. If the path contains spaces it must be provided in double quotes.
/D	Cancels the scan if this task has already been successful performed during this day.

Examples:

```
KAVSHELL FULLSCAN /WA:fullscan.log
```

9.3. Launching updates

Command syntax:

```
KAVSHELL UPDATE [updates_source] [/W[A][!]:report_file]
[/APP]
```

If no modifiers are specified, command syntax help will be displayed.

Modifier	Purpose
[updates_source]	An HTTP or an FTP server or a network folder used to download updates from. If the path is not specified, the updates source information will be borrowed from the anti-virus database and application modules updating task.

<pre> /W[A][!]: report_file /W: report_file /WA: report_file </pre>	<p>Logging events into the specified report_file:</p> <ul style="list-style-type: none"> • only important events; • all events. <p>Symbol ! is used to force the report file to overwritten each time the task is started.</p> <p>You can use either absolute or relative path to the file. If the path contains spaces it must be provided in double quotes.</p>
<pre> /APP </pre>	<p>Application modules update.</p>

Examples:

```

KAVSHELL UPDATE ftp://ftp.kaspersky.com/
/WA:avbases_upd.txt
KAVSHELL UPDATE /APP

```

9.4. Last update rollback

Command syntax:

```

KAVSHELL ROLLBACK [/W[A][!]:report_file]

```

If no modifiers are specified, command syntax help will be displayed.

Modifier	Purpose
<pre> /W[A][!]: report_file /W: report_file /WA: report_file </pre>	<p>Logging events into the specified report_file:</p> <ul style="list-style-type: none"> • only important events; • all events. <p>Symbol ! is used to force the report file to overwritten each time the task is started.</p> <p>You can use either absolute or relative path to the file. If the path contains spaces it must be provided in double quotes.</p>

Examples:

```

KAVSHELL ROLLBACK /WA:rollback.log

```

9.5. Starting the application

Command syntax:

```
KAVSHELL START
```

9.6. Stopping the application

Command syntax:

```
KAVSHELL STOP /PWD:password
```

Modifier	Purpose
/PWD:password	Entering the administrator's password required in order to execute the command.

Example:

```
KAVSHELL STOP /PWD:password
```

9.7. Managing tasks

Command syntax:

```
KAVSHELL TASK [ taskid {/START [/W[A][!]:report_file]|
                /STOP |
                /PAUSE |
                /RESUME [/W[A][!][: report_file]]|
                /DELETE } ] /PWD:password
```

If no modifiers are specified, command syntax help will be displayed along with unique identifiers and the status of each task.

Modifier	Purpose
/START	Starts a task with the specified identifier.

<pre> /W[A][!]:report_file /W:report_file /WA:report_file </pre>	<p>Logging events into the specified report_file:</p> <ul style="list-style-type: none"> • only important events; • all events. <p>Symbol ! is used to force the report file to be overwritten each time the task is started.</p> <p>You can use either absolute or relative path to the file. If the path contains spaces it must be provided in double quotes.</p>
<pre> /STOP </pre>	<p>Stops the task with the specified identifier.</p>
<pre> /PAUSE </pre>	<p>Pauses the task with the supplied identifier.</p>
<pre> /RESUME </pre>	<p>Resumes the task with the supplied identifier.</p>
<pre> /DELETE </pre>	<p>Deletes the task with the supplied identifier.</p>
<pre> taskid </pre>	<p>Unique task identifiers.</p> <p>You can manage system tasks using the following standard identifiers:</p> <ul style="list-style-type: none"> • scan-computer – full computer scan; • scan-removable – scan removable drives; • scan-quarantine – scan quarantine; • scan-critical – scan boot disk sectors, memory, startup objects; • update-bases – update anti-virus database; • update-app – update application modules; • rollback – rollback the last anti-virus database update;
<pre> /PWD:password </pre>	<p>Entering the administrator's password required to execute a command</p>

Examples:

```
KAVSHELL TASK /PWD:password
```

```
KAVSHELL TASK update-app /START /WA:fullscan.log
/PWD:password
KAVSHELL TASK _LOCAL_0630cddf-0793-4c2d-be1e-a3daed0904c6
/DELETE /PWD:password
```

9.8. Import/export of settings

Command syntax:

```
KAVSHELL IMPORT settings_file /PWD:password
KAVSHELL EXPORT settings_file /PWD:password
```

Modifier	Purpose
settings_file	The name of the profile file from which the Kaspersky Anti-Virus settings are imported (or into which they are imported). Details about profiles see section 5.8.3 on page 83).
/PWD:password	Entering the administrator's password required in order to execute the command.

Examples:

```
KAVSHELL IMPORT c:\kav50settings.xml /PWD:password
KAVSHELL EXPORT c:\kav50settings.xml /PWD:password
```

9.9. Adding a license key

Command syntax:

```
KAVSHELL ADDKEY file [/R] /PWD:password
```

Modifier	Purpose
file	License key file name.
[/R]	Replacing the current license key with a new key.
/PWD:password	Entering the administrator's password required in order to execute the command.

Example:

```
KAVSHELL ADDKEY c:\00A531D2.key /R /PWD:password
```

CHAPTER 10. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to the most frequently asked questions from users pertaining to installation, setup and operation of the Kaspersky Anti-Virus; here we shall try to answer them here in detail.



Question: Is it possible to use Kaspersky Anti-Virus with anti-virus products of other vendors?

We recommend uninstalling anti-virus products of other vendors prior to installation of Kaspersky Anti-Virus to avoid software conflicts.



Question: Kaspersky Anti-Virus does not rescan files that have been scanned earlier. Why?

This is true. Kaspersky Anti-Virus does not rescan files that have not changed since the last scan.

That has become possible due to new iChecker and technologies. The technology is implemented in the program using a database of file checksums.



Question: Why does Kaspersky Anti-Virus cause a certain decrease in server performance, noticeably loading the CPU?

Virus detection is a computationally intensive mathematical problem requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by Kaspersky Anti-Virus, and each new virus added to the anti-virus database increases the overall scanning time. This is a necessary sacrifice for the security and safety of your data.

Other anti-virus products speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor, and file formats that require complicated analysis (e.g. PDF) from their databases.

In contrast, Kaspersky Lab believes that the purpose of Kaspersky Anti-Virus is to establish real and complete anti-virus security for its users. We believe that "partial protection" is even worse than no protection at all, because it forces users to take personal precautions.

Kaspersky Anti-Virus gives its users maximum protection. Experienced users can, of course, accelerate anti-virus scanning to the detriment of overall security by disabling scanning of various file types, but we do not recommend doing so for users who want the best protection.

For maximum user protection, Kaspersky Anti-Virus recognizes more than 1200 formats of archived and compressed files and provides disinfection of 6 of them. This is essential for anti-virus security, because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one. This is achieved through the use of new unique technology iChecker™ developed at Kaspersky Lab.



Question: Why do I need the key file? Will my copy of Kaspersky Anti-Virus work without it?

No, Kaspersky Anti-Virus does not work without a license key.

If you are still undecided whether or not to purchase Kaspersky Anti-Virus, you can download a trial version of the application from the Kaspersky Lab's website, section **Downloads** → **Trial Version**. Such trial version will work for 15 days. When this period expires, the key will be blocked.



Question: What happens when the license expires?

After expiration of the license, Kaspersky Anti-Virus will continue operating, but anti-virus database updating will be disabled. Kaspersky Anti-Virus will continue cleaning infected objects but only using the old anti-virus database.

If such a situation arises, notify your system administrator and contact the company from which purchased Kaspersky Anti-Virus or Kaspersky Lab directly for license extension.



Question: Why should I perform updates on a daily basis?

A few years ago viruses were transmitted on floppy disks, and adequate computer protection could be achieved by installation of an anti-virus program followed by rare updates to its anti-virus database. However, recent virus epidemics spread around the world in several hours, and Kaspersky Anti-Virus with old database may be helpless against a new

threat. In order to resist new viruses, you should update the anti-virus database on a daily basis.

Each year Kaspersky Lab increases the frequency of its issued updates to the anti-virus database. Currently it is updated every hour.

Updating of the Kaspersky Anti-Virus application modules is an additional feature that allows both correction of discovered vulnerabilities and addition of new functions.



Question: *What are the changes to the updating service of version 5.0?*

The Kaspersky Lab 5.0 product suite features a new updating service which has been developed in accordance with the requests of our users. It automates the whole updating procedure, from the preparation of updates in Kaspersky Lab to the moment that relevant files are updated on clients' computers.

Advantages of the new updating service include:

- *Ability to resume downloading of files after disconnection.* Upon reconnection only files which have not been downloaded are retrieved.
- *Cumulative updates are now half the size.* A cumulative update contains the whole anti-virus database, therefore its size exceeds considerably the size of typical updates. The new service employs a special technology which allows using already existing anti-virus database for a cumulative update.
- *Accelerated downloading from the Internet.* Kaspersky Anti-Virus picks up a Kaspersky Lab's updates server located in your region. Furthermore, servers are allocated according to their performance, so you will not be sent to an overloaded server while there is another idle server available.
- *Use of key «black lists».* Unlicensed and illegal users are now prevented from using the updating service. Licensed users therefore do not suffer from inability to contact overloaded updates' servers.
- Corporate enterprises can now create a local updates' server. This feature is designed for organizations where a single LAN unites computers protected by Kaspersky Lab products. Any computer on the LAN can be turned into an updates' server that retrieves updates from the Internet and shares them with the other networked computers.



Question: *Is it possible for an intruder to replace the anti-virus database?*

Every anti-virus database has a one-of-a-kind signature checked by Kaspersky Anti-Virus when accessing the database. If the signature is wrong or the date of the database is later than that of the license expiration, Kaspersky Anti-Virus will not use it.



Question: *How should I set up updating for a single computer from the Internet, to enable further sharing of those updates with other networked computers?*

Let us refer to the computer to be updated from the Internet as the server, and to other computers as clients of that server.

You can use several methods to set up updating in a local area network:

- Enable use of a local updates' source within Kaspersky Administration Kit 5.0 server.
Kaspersky Administration Kit has built-in functionality for distribution of updates within corporate networks. It can update a shared source of updates according to a specified schedule and launch updating tasks on other computers. Kaspersky Administration Kit will check that the volume of data downloaded from the Internet does not exceed the actual needs of the installed applications. You can review the list of available patches on the server. The setup procedure is described in detail in the administrator's guide for Kaspersky Administration Kit 5.0.
- Enable use of a local updates' source in one of Kaspersky Lab products.
This option should be used when you cannot employ Kaspersky Administration Kit, or when you need to arrange a more complicated structure of updates' server networks.
In order to do so:
 - Identify the computers which will act as servers of updates. They should have Kaspersky Lab applications (version 5.0) installed.
 - Create a network resource to be used for further sharing of updates on each of the selected computers. It can be a network folder on a Microsoft Windows computer, FTP or HTTP server. Please define correct access rights for that folder.

- Create a new updating task or modify an existing one. Enable the sharing of updates through a local source and specify the created folder.
- Specify the local updates folder of the server as the source of updates on all computers, which should be updated from that server.



Question: *I use a proxy server and the updater does not work on my computer. What should I do?*

The following problems may cause inability to retrieve updates while working through a proxy server:

- Incorrect network settings.

There are two options for entering network settings when setting up the updating service: you may use Microsoft Internet Explorer settings or custom settings. The updating service sometimes incorrectly uses Microsoft Internet Explorer settings. This may occur in the following cases:

Internet connection is not set up on a computer;

Microsoft Internet Explorer settings are unavailable if none of the users has logged in;

proxy server requires authorization.

In all these cases, you should specify your network parameters directly in the settings of the update service.

- Proxy server being used belongs to a type unsupported by the updating service of Kaspersky Anti-Virus.

The updating service does not work through Kerio WinRoute, since WinRoute does not completely support HTTP 1.0 protocol. In this case, it is recommended to use any other proxy server.

The updating service also cannot work through Microsoft ISA Server using FTP protocol. In this case, we recommend obtaining updates from the Kaspersky Lab servers using HTTP protocol.



Question: *After Kaspersky Anti-Virus was installed, my operating system started behaving strangely (blue screen, computer restarting repeatedly, etc.) What should I do?*

This situation, although rare, is possible if there is a conflict between Kaspersky Anti-Virus and other software installed on your computer. In order to restore the functionality of your operating system:

1. As your computer starts loading press the **F8** key until the operating system loading options are displayed on your screen.
2. Select the **Safe mode** item and load the operating system.
3. Start Kaspersky Anti-Virus.
4. In the main application window switch to the **Settings** tab and press the [Additional Settings](#) link.
5. In the **Additional settings** dialog box that will open switch to the **Security** tab (see Figure 48) and uncheck the **Launch Kaspersky Anti-Virus at the system startup** box. Press the **OK** button.
6. Restart the operating system in the normal mode.

After this contact the Technical support service by visiting Kaspersky Lab's corporate website (section **Services** → **Technical Support** → **Send a question to the support service**). Describe your problem and conditions under which it occurs in as much detail as possible.

Make sure that you attach to your question a file containing a complete dump of Microsoft Windows operating system. In order to create this file, do the following:

1. Right-click **My computer** icon and select the **Properties** item in the shortcut menu that will open.
2. Select the **Advanced** tab in the **System Properties** window and then press the **Settings** button in the **Startup and Recovery** section.
3. Select the **Complete memory dump** option from the drop-down list in the **Write debugging information** section of the **Startup and Recovery** window.

By default, the dump file will be saved into the system folder as *memory.dmp*. You can change the dump storage folder by editing the folder name in the corresponding field.

4. Reproduce the problem related to the operation of Kaspersky Anti-Virus.
5. Make sure that the complete memory dump file was successfully saved.

APPENDIX A. CONTACTING TECHNICAL SUPPORT SERVICE

Kaspersky Anti-Virus provides support through Technical Support Service at Kaspersky Lab in the following cases:

- You believe that the application behaves abnormally and malfunctions.
- Kaspersky Anti-Virus has detected a suspicious file containing information valuable to you and has blocked it. You would like to continue working with the file.

If, while using Kaspersky Anti-Virus, you encountered problems, first of all you will have to check whether the method for solving your problem is described in the documentation, particularly, in section Frequently Asked Questions (see Chapter 10 on page 150) or in section **Services/Knowledge base** at the Kaspersky Lab's website (www.kaspersky.com).

If you have not found solution for your problem in the documentation and in the online Knowledge base, we recommend that you contact Kaspersky Lab's technical support service.

If you have a problem that must be solved immediately, call phone numbers specified in section C.2 on page 174. Phone support is provided 24/7 in Russian, English, French and German. Please pay attention that in order to obtain help, you must have a status of a registered user and provide to the Technical Support service representative your registration number (if you purchased a retail box version) or information on your order (if you purchased the product via the internet).



In order to send a message about application malfunctions to the Technical Support Service,

use the [Send question to tech support](#) hyperlink in the left frame of the **Support** tab (see Figure 4) in the main program window.

This will automatically open Kaspersky Lab's website with the Technical Support request form. You have to fill out this form. In the first window of the form provide information about the problem and the Kaspersky Anti-Virus license details.

- Select the **Type of question** by selecting in the dropdown list the particular problem you have encountered while using Kaspersky Anti-Virus.

- Select **Kaspersky Anti-Virus SOS** as the name of the Kaspersky Lab's product and provide a detailed description of the problem you encounter in the **Detailed description of your question** field.
- Select the type of the application registration by indicating the **license key** if you purchased the product in the box and installed the license key from a disk or **online purchase** if you purchased the application online.
- Enter the serial number of the license in the **License serial number or online order** field. You can find this information in the **Number** field in the **Managing license keys** window (see Figure 84).
- Enter your e-mail address in the **Your e-mail address** field.
- Press the **Next** button.

In the next window of the form provide general information about the software, hardware and peripherals of your computer. You can enter this information manually using the corresponding fields of the form or use a special automatic information service. In order to do it make sure that your browser allows running ActiveX objects and press the **Fill-in** button. Additionally, provide the following information:

- If, while using Kaspersky Anti-Virus SOS, you encountered a problem related to its compatibility with another application, please indicate the name of such application in the **Detected incompatibilities** field.
- Indicate your contact details in the **Contact information** section so that we can contact you in order to help you resolve this problem as soon as possible.
- Enter a special numeric code displayed in the **Protection against automatic registration** field to the left of the code and press the **Send question** button.

You can change the e-mail address that will be used your questions to the Technical Support service in the **General** tab (see Figure 46) in the Kaspersky Anti-Virus additional settings window (you can, for example, enter the security administrator's address), or specify the URL to be opened when you require technical support.

If Kaspersky Anti-Virus has quarantined a suspicious file, you may update the anti-virus database and attempt disinfecting it (see section 5.8.1.2 on page 74). However, if the object cannot be disinfecting, but you wish to recover it as soon as possible, you may send the object for examination to Kaspersky Lab. The file may really be infected with an unknown virus type or a false alarm might have occurred.



Attention! You can send suspicious files to Kaspersky Lab only if they were scanned using the anti-virus database updated on the day you are sending this file.



In order to send a suspicious file for examination to Kaspersky Lab,

select the suspicious file in the **Quarantine** window (see section 5.8.1.2 on page 74) and use the [Send to Kaspersky Lab for analysis](#) hyperlink.

Clicking the hyperlink will automatically open a window of the mail client installed on your computer, e.g. Microsoft Outlook Express, and create an e-mail message with the suspicious file attached. Send the message. Experts at Kaspersky Lab will closely examine the file you have sent and attempt to recover all the data in it. You will receive a full report regarding the results of file examination.



Please note that you may send no more than three files to Kaspersky Lab for examination within one day. Each file must have been scanned by Kaspersky Anti-Virus with a database updated no more than three days before the dispatch.

It may happen that Kaspersky Anti-Virus does not detect files that you are absolutely confident are infected with a new virus type during scanning. Such files can also be sent to Kaspersky Lab for analysis.



In order to send the files which you suspect of virus infection for analysis at Kaspersky Lab,

use the [Send file for analysis](#) hyperlink in the left frame of the **Support** tab (see Figure 4). Indicate the suspicious files in the standard browsing window.

The procedure of sending an e-mail message to Kaspersky Lab is absolutely identical to the one described for sending suspicious quarantined objects.

APPENDIX B. GLOSSARY

These documents use terms and concepts specific to the field of anti-virus protection. This glossary serves as a dictionary containing definitions for those concepts. For convenience, the glossary is arranged in alphabetic order.

A

Administration agent – a special application which provides for interaction between an administration server and applications from the corporate products of Kaspersky Lab. It is included in Kaspersky Administration Kit 5.0.

Administration console – a component providing a graphic interface for managing Kaspersky Anti-Virus. Included in Kaspersky Administration Kit 5.0.

Administration group – a number of computers combined into a group for convenient control. The group is managed as a whole entity, may have a group policy, may include other groups, and may receive administration commands.

Administration server – a special application functioning as a controller and centralized data storage for Kaspersky Lab applications installed on a corporate network. It is included in Kaspersky Administration Kit 5.0.

AdWare – software code for advertisement demonstration added into a program without informing the users about that. As a rule, adware is built into free software. The advertisement appears within the program interface. Such programs frequently collect and transmit to their developers some personal information about users, change various browser parameters (home and search pages, security levels, etc.), generating additional traffic, which users do not control. All of the above may cause violations of the security policy or even direct financial losses.

Anti-virus database – a database created by Kaspersky Lab specialists that contains detailed descriptions of all currently existing viruses and methods for their detection and disinfection. Our anti-virus database is regularly updated with information about new viruses; therefore, to keep your computer constantly protected from viruses, you need to keep your anti-virus database updated.

Anti-virus protection status – current status of anti-virus protection that characterizes the security level for your computer.

Application management plug-in – a specialized component which provides an interface for remote control of application through an administration console. Each application requires its own application management plug-in; therefore, it is included in the packages of all

Kaspersky Lab applications which can be controlled via Kaspersky Administration Kit 5.0.

Application modules – files, included into the distribution kit of Kaspersky Anti-Virus 5.0 SOS, and ensuring implementation of the main tasks of the application. For each type of tasks implemented by Kaspersky Anti-Virus (*real-time protection, on-demand scan, updates*) there is a corresponding executable module. When you start a full scan of your computer from the main application window, you launch a module corresponding to this task.

Available updates – Service Packs containing a collection of urgent updates and modifications to the application architecture, accumulated over a specified period of time.

B

Backing up – creating a backup of a file in the backup storage before treating it (disinfection or deleting). This file can later be restored from its backup, for example, for subsequent scanning with the current version of the anti-virus database.

Backup storage – a special storage area designed to preserve backup copies of objects made prior to their disinfection or removal.

"Black list" – the database containing the information about license keys belonging to owners who have committed violations of the License Agreement, and about keys that have been generated but remained unsold for some reason. The content of the black list is updated along with anti-virus databases; Kaspersky Anti-Virus will not work without it.

C

Centralized application control – application control performed through administration services provided by Kaspersky Administration Kit 5.0.

Current license key - the license key installed and currently used by Kaspersky Anti-Virus to unlock its functionality. It determines the period of license validity and licensing policy regarding the product. An application cannot have more than one key with "current" status.

D

Deleting an object – a method of treating an object. To delete an object is to remove it physically from a computer. This method is recommended for treating infected objects. If deleting is the first action applied to an object, it is necessary to create a backup copy of this object before deleting it. You can use the backup to restore the original object.

Disinfection – a method of treating *infected objects*. Disinfection implies partial or full recovery of data or results in a decision that these files cannot be disinfected. Objects are disinfected using the anti-virus database. If disinfection is the first action to be applied to an object, i. e. the first action after detection of a suspicious object, the application

creates a backup copy of this file. If some data are lost during disinfection, you can use the backup to recover this object.

Disinfection of objects at restart – a method of processing infected objects which are being accessed by other applications while the application attempts their disinfection. The application creates a copy of the infected object, disinfects the copy, and substitutes it for the original infected object during the next restart. In Microsoft Windows 9x operating systems disinfection of objects with long filenames during restart forces their replacement with disinfected objects having short filenames. That may cause incorrect functioning of applications, which use objects disinfected in this manner.

E

E-mail databases – databases that contain e-mail messages stored on your computer. Every incoming/outgoing message is saved in the database after you receive/send it. Such databases are scanned in the on-demand scanning mode.

Exclusions – user-defined settings that exclude certain objects from the scan. Thus, you can disable scanning of archives during a full scan or exclude files from scans by using masks.

Extended anti-virus database – *standard database* plus additional database that help detect potentially dangerous software on the user's computer.

F

File mask – is a representation of the name and the extension of a file using general symbols. Two main symbols used in the file masks are "*" and "?" (where "*" is any number of symbols and "?" is any single symbol). You can represent any file using these symbols. Please note that when providing the name and the extension of the file a dot notation is always used.

Full scan – a mode of application functioning designed for full computer scanning for the presence of malicious code upon a request made by a user with subsequent disinfection and removal of suspicious or infected objects, if any.

G

Group policy – a collection of parameters for application functionality in an administration group controlled via Kaspersky Administration Kit 5.0.

H

Hack Tools – software employed by intruders for their own purposes to gain access to your computer. The category includes various illegal scanners of vulnerabilities, password cracking tools, other types of software for breaking into network resources or intrusion into an attacked system.

High speed – a level of computer security which provides top system performance with some reduction in the number of objects scanned.

I

iChecker™ – the technology which allows the application to skip rescanning objects which are unchanged since their previous scanning. The technology is implemented using a database of object checksums.

Infected object – an object containing harmful code. We recommend that you abandon working on these objects because they can infect your computer.

J

Jokes – software that does not inflict any damage to the computer directly, but display messages falsely informing the user that this damage has been inflicted or will be inflicted under certain conditions. These programs often warn user about a danger that does not exist, for example they display messages about hard drive formatting (although no formatting is taking place), “detect” viruses in files that are not infected, etc.

K

Kaspersky Administration Kit 5.0 – an application included in Kaspersky Business Optimal and Kaspersky Corporate Suite and designed for centralized administration of an anti-virus protection system in a corporate network built on the basis of Kaspersky Lab applications.

Kaspersky Lab update servers – a list of http- and ftp-servers belonging to Kaspersky Lab from which Kaspersky Anti-Virus copies the anti-virus database and application module updates to your computer.

L

License key – a file with the .key extension that serves as your personal “key”. This file is required for correct operation of Kaspersky Anti-Virus. The license key is included in the distribution kit if you purchased your copy of Kaspersky Anti-Virus from Kaspersky Lab distributors. If you purchased the product online, the license key is sent to you via e-mail. Without the license key, Kaspersky Anti-Virus DOES NOT WORK.

License period – the period during which you have the right to use the full functionality of Kaspersky Anti-Virus. As a rule, the license period defined by the license key is one calendar year from the date of license key activation. After your license expires, the product will operate, but you will not be able to update the *anti-virus database* and *application modules*.

Logical network administrator – person who controls the operation of the application via the Kaspersky Administration Kit remote centralized administration system.

M

Maximum protection – the level of computer security which corresponds to maximum possible protection, leading to a certain performance decrease.

O

Object blocking – denying access to an object to external applications. A blocked object cannot be accessed for reading, execution, modification or removal.

OLE object – objects or documents embedded in other files using the OLE technology.

Q

Quarantine – a special data storage designed for isolation of suspicious objects.

Quarantining (moving to a quarantine folder) – a method for treating a *suspicious object* which involves blocking access to the object and moving it to a quarantine folder for subsequent treatment.

R

Recommended level – the default level of anti-virus protection with settings recommended by Kaspersky Lab experts which ensures the optimal balance between performance and protection.

Recovering, restoring – moving an original file from the *quarantine* or *backup* folders to a specified destination folder or to its original location, where it was stored before quarantining, disinfection, or deleting.

Reserved license key - a license key which has been installed to enable proper functionality of Kaspersky Anti-Virus but has not yet been activated. This reserved key will be activated as soon as the license provided by the current key expires.

Riskware – programs that are not viruses but yet impose a potential threat. Under some conditions the presence of such programs on the computer will present risk to your data. Such programs include remote administration software, automatic dialers connecting your to internet pay-sites using dial-up connection, etc.

Rootkit – utilities used to conceal the malicious actions. They “hide” malware so that it is not detected by anti-virus programs. Rootkits can also modify the operating system altering its main functions to conceal their presence and actions performed by the malefactor on the infected computer.

S

Scan infectable files, by extension – when scanning, the application takes into account file extension.

Security administrator –person who controls the operation of the application. The administrator may either act remotely using *Administration Console* or using a local interface.

Settings file – a file containing basic program settings. Software settings can be exported (saved) to such files or imported (loaded) from file.

SpyWare – software designed for unauthorized access to user data, tracking of actions performed on a computer, collection of information about hard drive contents. Such tools allow an intruder to gather data or even control a computer from outside. Spyware is usually distributed with free software and deploy on a computer imperceptibly for its user. Spyware category includes software tracking keyboard input, password cracking tools, programs for collection of confidential data (e. g., credit card numbers).

Standard anti-virus database – anti-virus database that helps detect all malware existing at the moment and disinfect objects and data infected such malware.

Startup objects – a set of programs that are necessary for launching and correct operation of the operating system and other programs installed on your computer. Your operating system launches these objects during each startup. Some viruses attempt to infect the startup objects and can cause a startup failure.

Suspicious object – an object that contains either a modified code of a well-known virus or a code reminiscent of a virus, but not yet known to Kaspersky Lab.

T

Task – a specific action performed by an application of Kaspersky Lab.

U

Unknown virus – a new virus that is not recorded in the *anti-virus database*. As a rule, Kaspersky Anti-Virus detects unknown viruses using an *heuristic code analyzer* and objects containing these viruses are identified as *suspicious*.

Update – the procedure of replacement/addition of new files (the anti-virus databases or application modules) downloaded from Kaspersky Lab update servers.

Urgent updates – critical updates of application modules.

V

Virtual drives (RAM drives) – RAM area in a personal computer which emulates a regular physical computer disk.

APPENDIX C. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

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

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

C.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal has been designed to provide anti-virus protection to personal computers running Microsoft Windows 98/ME or Microsoft Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, Internet, floppy disks, CD, etc. The unique system of heuristic data analysis allows efficient neutralization of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scanning and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had already been scanned during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This feature **considerably increases the speed of the program's operation**.

The application creates a reliable barrier against viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocols and provides highly efficient detection of viruses in mail databases.

The application supports over 700 formats of archived and compressed files and provides automatic scanning of their content as well as removal of malicious code from **ZIP, CAB, RAR, ARJ, LHA** and **ICE** archives.

Configuring the application is made simple and intuitive due to the possibility to select one of three preset protection levels: **Maximum Protection, Recommended** or **High Speed**.

The anti-virus database is updated every hour and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the Internet or the connection has to be changed.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Microsoft Windows 98/ME, Microsoft Windows 2000/NT, Microsoft Windows XP as well as MS Office applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic

retrieval of daily updates for the anti-virus database and the program modules. A unique second-generation heuristic analyzer efficiently detects unknown viruses. A simple and convenient interface allows users to configure the program quickly making work with it easier than ever.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks.
- **Real-time automatic protection** of all accessed files from viruses.
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases.
- **Behavior blocker** that provides maximum protection of MS Office applications against viruses.
- **Archive scanning** – Kaspersky Anti-Virus recognizes over 900 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP, CAB, RAR, ARJ, LHA** and **ICE** archives.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Microsoft Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, Kaspersky® Anti-Hacker blocks the suspicious application from accessing the network. This helps ensure enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite is a software suite designed for organizing comprehensive protection of personal computers running Microsoft Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection of data saved on your computer
- protection against spam for users of Microsoft Outlook and Microsoft Outlook Express
- protection of your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, for notifications about the current status of virus activity and fresh news. The program reads the list of available news channels and their content from news server of Kaspersky Lab with specified frequency.

The product performs the following functions:

- It visualizes in the system tray the current status of virus activity.
- The product allows the users to subscribe and unsubscribe from news channels.
- It retrieves news from each subscribed channel with the specified frequency and notifies about fresh news.
- It allows reviewing news on the subscribed channels.
- It allows reviewing the list of channels and their status.
- It allows opening pages with news details in your browser.

News Agent is a stand-alone Windows application, which can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

The program is a free service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus check of your computer. Kaspersky OnLine Scanner runs within your web browser using Microsoft ActiveX® technology. Thus, users can quickly test their computers in case of a slightest suspicion of malicious infection. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

Kaspersky® OnLine Scanner Pro

This program is a subscription service available to visitors of the corporate website allowing to perform efficient anti-virus scan of your computer and disinfection of infected files online. Kaspersky OnLine Scanner Pro is executed in the web browser using the Microsoft ActiveX® technology. While scanning the user can:

- exclude archives and mail databases from the scan scope;
- select standard / extended anti-virus database to be used for scanning;
- save reports with the scan results in txt and html format.

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, directories or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- **Control of changes within file system.** The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitoring of processes in random-access memory.** Kaspersky Anti-Virus 6.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in standard processes occur.

- **Monitoring of changes in OS registry** due to internal system registry control.
- **Blocking of dangerous VBA macros** in Microsoft Office documents.
- **System restoration** after malicious spyware influence accomplished due to recording of all changes in the registry and computer file system and an opportunity to perform their roll-back at user's discretion.

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 is an integrated solution for protection of personal computers against the main information-related threats, i.e. viruses, hackers, spam and spyware. A common user interface allows configuration and management of all solution components.

The anti-virus protection feature includes:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used. The program includes plug-ins for popular e-mail clients (Microsoft Office Outlook, Microsoft Outlook Express and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection:** anti-virus scanning of individual files, directories or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.
- **Proactive protection:** the program performs constant monitoring of application activity and processes running in random-access memory preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is guaranteed owing to the ability to recognize phishing attacks, which helps prevent confidential data leaks (first of all, your passwords, bank account and credit card numbers), and block execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The feature **blocking charged phone calls** helps identify software that attempts to use your modem for hidden unauthorized connection to paid phone services and prevents such activity.

Kaspersky® Internet Security 6.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical hacker attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth mode** (owing to the SmartStealth™ technology) **prevents**

computer detection from outside. When you switch into that mode, the system will block all network activity except for a few transactions allowed in user-defined rules.

The program employs complex approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites).
- Inspection of phrases in message body.
- Analysis of message text using a self-learning algorithm.
- Recognition of spam sent in image files.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of hand-held computers and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both in internal memory of PDA and smartphones or on memory cards of any type) on user demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a unique configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus protection⁴ for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux.
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers.

⁴ Depending on the type of distribution kit.

- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a unique tool for automated deployment and administration.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;
- *E-mail systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS, and also smartphones running Microsoft Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for anti-virus processing of e-mail transmitted via SMTP. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a number of tools reducing the load on the mail system and preventing hacker attacks. DNS Black List support provides protection against e-mails coming from servers entered in these lists as sources distributing unwanted e-mail (spam).

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange performs anti-virus processing of incoming and outgoing mail messages as well as messages stored at the server, including letters in public folders and filters out unsolicited correspondence using "smart" spam recognition techniques in combination with Microsoft technologies. The application scans all messages arriving at an Exchange Server via SMTP protocol checking them for the presence of viruses using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes. It filters out spam based on formal attributes (mail address, IP address, letter size, heading) and analyzes the content of messages and of their attachments using "smart" technologies, including unique graphic signatures for identifying graphic SPAM. The application scans both the message body and the attached files.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and

performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features.

C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. All of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: info@kaspersky.com

APPENDIX D. LICENSE AGREEMENT

End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD'S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) PURCHASED ON LINE FROM THE KASPERSKY LAB INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF 7 WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN

THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such

steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements

described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means:

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab.

You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Limitation of Liability.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage

(whether such losses or damage were foreseen, foreseeable, known or otherwise):

- (a) Loss of revenue;
- (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
- (c) Loss of the use of money;
- (d) Loss of anticipated savings;
- (e) Loss of business;
- (f) Loss of opportunity;
- (g) Loss of goodwill;
- (h) Loss of reputation;
- (i) Loss of, damage to or corruption of data, or:
- (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii) below, you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).