

KASPERSKY LAB

Kaspersky[®] Anti-Virus 6.0

USER GUIDE

KASPERSKY ANTI-VIRUS 6.0

User Guide

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

Revision date: January 2006

Table of Contents

| | |
|---|----|
| CHAPTER 1. THREATS TO COMPUTER SECURITY..... | 9 |
| 1.1. Sources of Threats | 9 |
| 1.2. How threats spread | 10 |
| 1.3. Types of Threats..... | 12 |
| 1.4. Signs of Infection | 15 |
| 1.5. What to do if you suspect infection | 16 |
| 1.6. Preventing Infection..... | 17 |
| CHAPTER 2. KASPERSKY ANTI-VIRUS 6.0..... | 19 |
| 2.1. What's new in Kaspersky Anti-Virus 6.0..... | 19 |
| 2.2. The elements of Kaspersky Anti-Virus Defense..... | 21 |
| 2.2.1. Protection components..... | 22 |
| 2.2.2. Virus scan tasks..... | 23 |
| 2.2.3. Program tools..... | 23 |
| 2.3. Hardware and software system requirements | 25 |
| 2.4. Software packages..... | 25 |
| 2.5. Support for registered users..... | 26 |
| CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS 6.0..... | 27 |
| 3.1. Installation procedure using the Installation Wizard | 27 |
| 3.2. Setup Wizard | 31 |
| 3.2.1. Using objects saved with Version 5.0 | 31 |
| 3.2.2. Activating the program..... | 31 |
| 3.2.2.1. Selecting a program activation method..... | 32 |
| 3.2.2.2. Entering the activation code | 32 |
| 3.2.2.3. Obtaining a license key..... | 33 |
| 3.2.2.4. Selecting a license key file..... | 33 |
| 3.2.2.5. Completing program activation..... | 33 |
| 3.2.3. Selecting a security mode | 33 |
| 3.2.4. Configuring update settings..... | 34 |
| 3.2.5. Configuring a virus scan schedule | 35 |
| 3.2.6. Restricting program access..... | 35 |

| | |
|---|----|
| 3.2.7. Application Integrity Control..... | 36 |
| 3.2.8. Finishing the Setup Wizard | 36 |
| 3.3. Installing the program from the command prompt | 36 |
| 3.4. Upgrading from 5.0 to 6.0 | 37 |
| CHAPTER 4. PROGRAM INTERFACE | 38 |
| 4.1. System tray icon | 38 |
| 4.2. The context menu..... | 39 |
| 4.3. Main program window | 40 |
| 4.4. Program settings window | 43 |
| CHAPTER 5. GETTING STARTED | 45 |
| 5.1. What is the protection status of my computer? | 45 |
| 5.1.1. Protection indicators | 46 |
| 5.1.2. Kaspersky Anti-Virus component status..... | 49 |
| 5.1.3. Program performance statistics | 50 |
| 5.2. How to scan your computer for viruses | 50 |
| 5.3. How to scan critical areas of the computer..... | 51 |
| 5.4. How to scan a file, folder or disk for viruses | 51 |
| 5.5. How to update the program | 52 |
| 5.6. What to do if protection is not running | 53 |
| CHAPTER 6. PROTECTION MANAGEMENT SYSTEM..... | 54 |
| 6.1. Stopping and resuming protection on your computer | 54 |
| 6.1.1. Pausing protection | 54 |
| 6.1.2. Stopping protection..... | 56 |
| 6.1.3. Pausing / stopping protection components, virus scans, and update tasks | 56 |
| 6.1.4. Restoring protection on your computer..... | 57 |
| 6.1.5. Shutting down the program | 58 |
| 6.2. Types of programs to be monitored..... | 58 |
| 6.3. Creating a trusted zone | 59 |
| 6.3.1. Exclusion rules | 60 |
| 6.3.2. Trusted applications..... | 65 |
| 6.4. Starting virus scan and update tasks under another user account | 68 |
| 6.5. Configuring virus scan and update schedules | 69 |
| 6.6. Power options | 71 |
| 6.7. Advanced Disinfection Technology | 72 |

| | |
|--|-----|
| CHAPTER 7. FILE ANTI-VIRUS | 73 |
| 7.1. Selecting a file security level | 73 |
| 7.2. Configuring File Anti-Virus..... | 75 |
| 7.2.1. Defining the file types to be scanned | 75 |
| 7.2.2. Defining protection scope | 78 |
| 7.2.3. Configuring advanced settings..... | 79 |
| 7.2.4. Restoring default File Anti-Virus settings | 82 |
| 7.2.5. Selecting actions for objects..... | 82 |
| 7.3. Postponed disinfection | 84 |
| CHAPTER 8. MAIL ANTI-VIRUS | 85 |
| 8.1. Selecting an email protection level | 86 |
| 8.2. Configuring Mail Anti-Virus..... | 87 |
| 8.2.1. Selecting a protected email group..... | 88 |
| 8.2.2. Configuring email processing in Microsoft Office Outlook..... | 89 |
| 8.2.3. Configuring email scans in The Bat! | 91 |
| 8.2.4. Restoring default Mail Anti-Virus settings | 92 |
| 8.2.5. Selecting actions for dangerous email objects | 93 |
| CHAPTER 9. WEB ANTI-VIRUS | 95 |
| 9.1. Selecting the web security level..... | 96 |
| 9.2. Configuring Web Anti-Virus..... | 98 |
| 9.2.1. Setting a scan method..... | 98 |
| 9.2.2. Creating a trusted address list..... | 99 |
| 9.2.3. Restoring default Web Anti-Virus settings | 100 |
| 9.2.4. Selecting responses to dangerous objects..... | 101 |
| CHAPTER 10. PROACTIVE DEFENSE | 102 |
| 10.1. Proactive Defense settings | 105 |
| 10.1.1. Activity control rules | 106 |
| 10.1.2. Application Integrity Control..... | 110 |
| 10.1.2.1. Configuring Application Integrity Control rules..... | 111 |
| 10.1.2.2. Creating a list of shared components..... | 113 |
| 10.1.3. Office Guard..... | 114 |
| 10.1.4. Registry Guard..... | 116 |
| 10.1.4.1. Selecting registry keys for creating a rule | 118 |
| 10.1.4.2. Creating a Registry Guard rule..... | 119 |

| | |
|--|-----|
| CHAPTER 11. SCANNING FOR VIRUSES ON YOUR COMPUTER | 121 |
| 11.1. Managing virus scan tasks..... | 122 |
| 11.2. Creating a list of objects to scan | 122 |
| 11.3. Creating virus scan tasks | 124 |
| 11.4. Configuring virus scan tasks | 125 |
| 11.4.1. Selecting a security level | 125 |
| 11.4.2. Specifying the types of objects to scan..... | 126 |
| 11.4.3. Restoring default scan settings | 129 |
| 11.4.4. Selecting actions for objects..... | 129 |
| 11.4.5. Advanced virus scan options | 131 |
| 11.4.6. Setting up global scan settings | 133 |
| CHAPTER 12. TESTING KASPERSKY ANTI-VIRUS FEATURES | 134 |
| 12.1. The EICAR test virus and its variations | 134 |
| 12.2. Testing File Anti-Virus | 136 |
| 12.3. Testing Virus scan tasks | 137 |
| CHAPTER 13. PROGRAM UPDATES..... | 139 |
| 13.1. Starting the Updater | 140 |
| 13.2. Rolling back to the previous update..... | 141 |
| 13.3. Creating update tasks | 141 |
| 13.4. Configuring update settings | 143 |
| 13.4.1. Selecting an update source..... | 143 |
| 13.4.2. Selecting an update method and what to update..... | 145 |
| 13.4.3. Configuring connection settings | 147 |
| 13.4.4. Update distribution | 149 |
| 13.4.5. Actions after updating the program..... | 150 |
| CHAPTER 14. ADVANCED OPTIONS | 152 |
| 14.1. Quarantine for potentially infected objects..... | 153 |
| 14.1.1. Actions with quarantined objects..... | 154 |
| 14.1.2. Setting up Quarantine..... | 155 |
| 14.2. Backup copies of dangerous objects..... | 156 |
| 14.2.1. Actions with backup copies | 156 |
| 14.2.2. Configuring Backup settings | 158 |
| 14.3. Reports | 158 |
| 14.3.1. Configuring report settings | 161 |

| | |
|---|------------|
| 14.3.2. The <i>Detected</i> tab | 161 |
| 14.3.3. The <i>Events</i> tab | 162 |
| 14.3.4. The <i>Statistics</i> tab | 163 |
| 14.3.5. The <i>Settings</i> tab | 164 |
| 14.3.6. The <i>Macros</i> tab | 165 |
| 14.3.7. The <i>Registry</i> tab | 166 |
| 14.4. General information about the program | 167 |
| 14.5. Managing licenses | 168 |
| 14.6. Technical Support | 170 |
| 14.7. Creating a monitored port list | 171 |
| 14.8. Checking your SSL connection | 173 |
| 14.9. Configuring the Kaspersky Anti-Virus interface | 175 |
| 14.10. Rescue Disk | 176 |
| 14.10.1. Creating a rescue disk | 177 |
| 14.10.1.1. Getting ready to write the disk | 177 |
| 14.10.1.2. Creating an .iso file | 178 |
| 14.10.1.3. Burning the disk | 178 |
| 14.10.1.4. Finishing creating a rescue disk | 178 |
| 14.10.2. Using the rescue disk | 178 |
| 14.11. Using advanced options | 180 |
| 14.11.1. Kaspersky Anti-Virus event notifications | 180 |
| 14.11.1.1. Types of events and notification delivery methods | 181 |
| 14.11.1.2. Configuring email notification | 183 |
| 14.11.1.3. Configuring event log settings | 184 |
| 14.11.2. Self-Defense and access restriction | 185 |
| 14.11.3. Resolving conflicts with other applications | 187 |
| 14.12. Importing and exporting Kaspersky Anti-Virus settings | 187 |
| 14.13. Resetting to default settings | 188 |
| | |
| CHAPTER 15. WORKING WITH THE PROGRAM FROM THE COMMAND PROMPT | 189 |
| 15.1. Activating the application | 190 |
| 15.2. Managing program components and tasks | 191 |
| 15.3. Anti-virus scans | 192 |
| 15.4. Program updates | 196 |
| 15.5. Rollback settings | 197 |
| 15.6. Exporting settings | 197 |

| | |
|--|-----|
| 15.7. Importing settings | 198 |
| 15.8. Starting the program..... | 199 |
| 15.9. Stopping the program..... | 199 |
| 15.10. Viewing Help..... | 199 |
| 15.11. Return codes from the command line interface | 200 |
| CHAPTER 16. MODIFYING, REPAIRING, AND REMOVING THE PROGRAM | 201 |
| 16.1. Modifying, repairing and removing the program using Setup Wizard | 201 |
| 16.2. Uninstalling the program from the command prompt..... | 203 |
| CHAPTER 17. FREQUENTLY ASKED QUESTIONS..... | 204 |
| APPENDIX A. REFERENCE INFORMATION | 206 |
| A.1. List of files scanned by extension..... | 206 |
| A.2. Possible file exclusion masks | 208 |
| A.3. Possible threat exclusion classifications from the Virus Encyclopedia | 209 |
| APPENDIX B. KASPERSKY LAB..... | 211 |
| B.1. Other Kaspersky Lab Products | 212 |
| B.2. Contact Us..... | 217 |
| APPENDIX C. LICENSE AGREEMENT | 218 |

CHAPTER 1. THREATS TO COMPUTER SECURITY

As information technology has rapidly developed and penetrated many aspects of human existence, so the number and range of crimes aimed at breaching information security has grown.

Cyber criminals have shown great interest in the activities of both state structures and commercial enterprises. They attempt to steal or disclose confidential information, which damages business reputations, disrupts business continuity, and may impair an organization's information resources. These acts can do extensive damage to assets, both tangible and intangible.

It is not only big companies who are at risk; individual users can also be attacked. Criminals can gain access to personal data (for instance, bank account and credit card numbers and passwords), or cause a computer to malfunction. Some types of attacks can give hackers complete access to a computer, which can then be used as part of a "zombie network" of infected computers to attack servers, send out spam, harvest confidential information, and spread new viruses and Trojans.

In today's world, it is widely acknowledged that information is a valuable asset which should be protected. At the same time, information must be accessible to those who legitimately require it (for instance, employees, clients and partners of a business). Hence the need to create a comprehensive information security system, which must take account of all possible sources of threats, whether human, man-made, or natural disasters, and use a complete array of defensive measures, at the physical, administrative and software levels.

1.1. Sources of Threats

A person, a group of people, or phenomena unrelated to human activity can threaten information security. Following from this, all threat sources can be put into one of three groups:

- **The human factor.** This group of threats concerns the actions of people with authorized or unauthorized access to information. Threats in this group can be divided into:
 - *External*, including cyber criminals, hackers, internet scams, unprincipled partners, and criminal organisations.

- *Internal*, including the actions of company staff and users of home PCs. Actions taken by this group could be deliberate or accidental.
- **The technological factor.** This threat group is connected with technical problems – use of obsolete or poor-quality software and hardware to process information. This can lead to equipment failure and often to data loss.
- **The natural-disaster factor.** This threat group includes the whole range of events caused by nature and independent of human activity.

All three threat sources must be accounted for when developing a data security protection system. This User Guide focuses on the area that is directly tied to Kaspersky Lab's expertise – external threats involving human activity.

1.2. How threats spread

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

The Internet

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

However, these very features of the worldwide web give hackers the ability to commit crimes on the Internet, and makes the hackers difficult to detect and punish.

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

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

Lastly, since it became possible to use credit cards and e-money through the Internet in online stores, auctions, and bank homepages, online scams have become increasingly common.

Intranet

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

Email

Since the overwhelming majority of computers have email client programs installed, and since malicious programs exploit the contents of electronic address books, conditions are usually right for spreading malicious programs. The user of an infected computer might, without realizing, send infected emails to friends or coworkers who in turn send more infected emails. For example, it is common for infected file documents to go undetected when distributed with business information via a company's internal email system. When this occurs, more than a handful of people are infected. It might be hundreds or thousands of company workers, together with potentially tens of thousands of subscribers.

Beyond the threat of malicious programs lies the problem of electronic junk email, or spam. Although not a direct threat to a computer, spam increases the load on email servers, eats up bandwidth, clogs up the user's mailbox, and wastes working hours, thereby incurring financial harm.

Also, hackers have begun using mass mailing programs and social engineering methods to convince users to open emails, or click on a link to certain websites. It follows that spam filtration capabilities are valuable for several purposes: to stop junk email; to counteract new types of online scans, such as phishing; to stop the spread of malicious programs.

Removable storage media

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

Opening a file that contains malicious code and is stored on a removable storage device can damage data stored on the local computer and spread the virus to the computer's other drives or other computers on the network.

1.3. Types of Threats

There are a vast number of threats to computer security today. This section will review the threats that are blocked by Kaspersky Anti-Virus.

Worms

This category of malicious programs spreads itself largely by exploiting vulnerabilities in computer operating systems. The class was named for the way that worms crawl from computer to computer, using networks, and email. This feature allows worms to spread themselves very rapidly.

Worms penetrate a computer, search for the network addresses of other computers, and send a burst of self-made copies to these addresses. In addition, worms often utilize data from email client address books. Some of these malicious programs occasionally create working files on system disks, but they can run without any system resources except RAM.

Viruses

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

Trojans

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

Recently, worms have been the commonest type of malicious program damaging computer data, followed by viruses and Trojans. Some malicious programs combine features of two or even three of these classes.

Adware

Adware comprises programs which are included in software, unknown to the user, which is designed to display advertisements. Adware is usually built into software that is distributed free. The advertisement is situated in the program interface. These programs also frequently collect personal data on the user and send it back to their developer, change browser settings (start page and search pages, security levels, etc.) and create

traffic that the user cannot control. This can lead to a security breach and to direct financial losses.

Spyware

This software collects information about a particular user or organization without their knowledge. Spyware often escapes detection entirely. In general, the goal of spyware is to:

- trace user actions on a computer;
- gather information on the contents of your hard drive; in such cases, this usually involves scanning several directories and the system registry to compile a list of software installed on the computer;
- gather information on the quality of the connection, bandwidth, modem speed, etc.

Riskware

Riskware includes software that does not have malicious features but could form part of the development environment for malicious programs or could be used by hackers as auxiliary components for malicious programs. This program category includes programs with backdoors and vulnerabilities, as well as some remote administration utilities, keyboard layout togglers, IRC clients, FTP servers, and all-purpose utilities for stopping processes or hiding their operation.

Another type of malicious program that is similar to adware, spyware, and riskware are programs that plug into your web browser and redirect traffic. The web browser will open different web sites than those intended.

Jokes

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

Rootkits

These are utilities which are used to conceal malicious activity. They mask malicious programs to keep anti-virus programs from detecting them. Rootkits modify basic functions of the computer's operating system to hide both their own existence and actions that the hacker undertakes on the infected computer.

Other dangerous programs

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

Hacker attacks

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

Some types of online scams

Phishing is an online scam that uses mass emailings to steal confidential information from the user, generally of a financial nature. Phishing emails are designed to maximally resemble informative emails from banks and well-known companies. These emails contain links to fake websites created by hackers to mimic the site of the legitimate organization. On this site, the user is asked to enter, for example, his credit card number and other confidential information.

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

Intrusive advertising

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

Spam

Spam is anonymous junk email, and includes several different types of content: adverts; political messages; requests for assistance; emails that ask one to invest large amounts of money or to get involved in pyramid schemes; emails aimed at stealing passwords and credit card numbers, and emails that ask to be sent to friends (chain letters).

Kaspersky Anti-Virus uses two methods for detecting and blocking these threat types:

- *Reactive* – this method searches for malicious files using a threat signature database that is regularly updated.
- *Proactive* – in contrast to reactive protection, this method is not based on analyzing code but on the system's behavior. This method is aimed at detecting new threats that are still not defined in the signatures.

By employing both methods, Kaspersky Anti-Virus provides comprehensive protection for your computer from both known and new threats.

1.4. Signs of Infection

There are a number of signs that a computer is infected. The following events are good indicators that a computer is infected with a virus:

- Unexpected messages or images appear on the screen or you hear unusual sounds;
- The CD/DVD-ROM tray opens and closes unexpectedly;
- The computer arbitrarily launches a program without your assistance;
- Warnings pop up on the screen about a program attempting to access the Internet, even though you initiated no such action;

There are also several typical traits of a virus infection through email:

- Friends or acquaintances tell you about messages from you that you never sent;
- Your inbox houses a large number of messages without return addresses or headers.

It must be noted that these signs can arise from causes other than viruses. For example, in the case of email, infected messages can be sent with your return address but not from your computer.

There are also indirect indications that your computer is infected:

- Your computer freezes or crashes frequently;
- Your computer loads programs slowly;
- You cannot boot up the operating system;
- Files and folders disappear or their contents are distorted;
- The hard drive is frequently accessed (the light blinks);

- The web browser program (for example, Microsoft Internet Explorer) freezes or behaves unexpectedly (for example, you cannot close the program window).

In 90% of cases, these indirect systems are caused by malfunctions in hardware or software. Despite the fact that such symptoms rarely indicate infection, we recommend that, upon detecting them, you run a complete scan of your computer (see 5.2 on pg. 50) with the settings at the **recommended** level.

1.5. What to do if you suspect infection

If you notice that your computer is behaving suspiciously...

1. Don't panic! This is the golden rule: it could save you from losing important data, and from a lot of needless worry.
2. Disconnect your computer from the Internet or local network, if it is on one.
3. If the computer will not boot from the hard drive (the computer displays an error message when you turn it on), try booting in safe mode or with the emergency operating system boot disk that you created when you installed the operating system.
4. Before doing anything else, back up your work on removable storage media (floppy, CD/DVD, flash drive, etc.).
5. Install Kaspersky Anti-Virus, if you have not done so already. See section Chapter 3 on page 27.
6. Update the program's threat signatures and application modules (see 5.5 on pg. 52). If possible, download the updates off the Internet from a different, uninfected computer, for instance at a friend's, an Internet café, or work. It is better to use a different computer since, when you connect an infected computer to the Internet, there is a chance that the virus will send important information to hackers or spread the virus to the addresses in your address book. That is why if you suspect that your computer has a virus, you should immediately disconnect from the Internet. You can also get threat signature updates on floppy disk from Kaspersky Lab or its distributors and update your signatures using the disk.
7. Select the security level recommended by the experts at Kaspersky Lab.
8. Start a full computer scan (see 5.2 on pg. 50).

1.6. Preventing Infection

Not even the most reliable and deliberate measures can provide 100% protection against computer viruses and Trojans, but following such a set of rules significantly lowers the likelihood of virus attacks and the level of potential damage.

The basic safety rules are discussed in the rest of this chapter..

Rule No. 1: *Use anti-virus software and Internet security programs.* To do so:

- Install Kaspersky Anti-Virus as soon as possible.
- Regularly (see 5.5 on pg. 52) update the program's threat signatures. You should update the signatures several times per day during virus outbreaks. In such situations, the threat signatures on Kaspersky Lab's update servers are updated immediately.
- Select the security settings recommended by Kaspersky Lab for your computer. You will be protected constantly from the moment the computer is turned on, and it will be harder for viruses to infect your computer.
- Select the settings for a complete scan recommended by Kaspersky Lab, and schedule scans for at least once per week.

Rule No. 2: *Use caution when copying new data to your computer.*

- Scan all removable storage drives, for example floppies, CD/DVDs, and flash drives, for viruses before using them (see 5.4 on pg. 51).
- Treat emails with caution. Do not open any files attached to emails unless you are certain that you were intended to receive them, even if they were sent by people you know.
- Be careful with information obtained through the Internet. If any web site suggests that you install a new program, be certain that it has a security certificate.
- If you are copying an executable file from the Internet or local network, be sure to scan it with Kaspersky Anti-Virus.
- Use discretion when visiting web sites. Many sites are infected with dangerous script viruses or Internet worms.

Rule No. 3: *Pay close attention to information from Kaspersky Lab.*

In most cases, Kaspersky Lab announces a new outbreak long before it reaches its peak. The likelihood of the infection in such a case is low, and

once you download the threat signature updates, you will have plenty of time to protect yourself against the new virus.

Rule No. 4: *Do not trust virus hoaxes*, such as prank programs and emails about infection threats.

Rule No. 5: *Use the Windows Update tool* and regularly install Windows operating system updates.

Rule No. 6: *Buy legitimate copies of software from official distributors.*

Rule No. 7: *Limit the number of people who are allowed to use your computer.*

Rule No. 8: *Lower the risk of unpleasant consequences of a potential infection:*

- Back up data regularly. If you lose your data, the system can fairly quickly be restored if you have backup copies. Store distribution floppies, CDs, flash drives, and other storage media with software and valuable information in a safe place.
- Create a Rescue Disk (see 14.10 on pg. 176) that you can use to boot up the computer, using a clean operating system.

Rule No. 9: *Regularly inspect the list of installed programs on your computer.* To do so, open **Install/Remove Programs** in the **Control Panel**, or look through the **Program Files** directory and the startup directory. You may discover software here that was installed on your computer without your knowledge, for example, while you were using the Internet or installing a different program. Programs like these are almost always potentially dangerous.

CHAPTER 2. KASPERSKY ANTI-VIRUS 6.0

Kaspersky Anti-Virus 6.0 heralds a new generation of data security products.

What really sets Kaspersky Anti-Virus 6.0 apart from other software, even from other Kaspersky Lab products, is its multi-faceted approach to data security.

2.1. What's new in Kaspersky Anti-Virus 6.0

Kaspersky Anti-Virus 6.0 (henceforth referred to as “Kaspersky Anti-Virus”, or “the program”) has a new approach to data security. The program's main feature is that it combines and noticeably improves the existing features of all the company's products in one security solution. The program provides protection against viruses and unknown threats.

You will no longer need to install several products on your computer for overall security. It is enough simply to install Kaspersky Anti-Virus 6.0.

Comprehensive protection guards all incoming and outgoing data channels. All of the program's components have flexible settings which enable Kaspersky Anti-Virus to adapt to the needs of each user. Configuration of the entire program can be done from one location.

Let's take a look at the new features in Kaspersky Anti-Virus.

New Protection Features

- Kaspersky Anti-Virus protects you both from known malicious programs, and from programs that have not yet been discovered. Proactive Defense (see Chapter 10 on pg. 102) is the program's key advantage. It analyzes the behavior of applications installed on your computer, monitoring changes to the system registry, tracking macros, and fighting hidden threats. The component uses a heuristic analyzer to detect and record various types of malicious activity, with which actions taken by malicious programs can be rolled back and the system can be restored to its state prior to the malicious activity.
- File Anti-Virus technology has been improved: now you can lower the load on the central processor and disk subsystems and increase the

speed of file scans. iChecker™ and iSwift™ help achieve this. This method rules out the application repeating scans of the same files.

- The scan process now runs as a background task, enabling the user to continue using the computer. If there is a competition for system resources, the virus scan will pause until the user's operation is completed and then resumes at the point where it left off.
- Critical areas of the computer, which if infected would seriously affect data quality or security, are given their own separate task. This task can be configured to run automatically every time the system is started.
- Major advances have been made in protecting the user's e-mail from malicious programs. The program scans these protocols for emails containing viruses:
 - IMAP, SMTP, POP3, regardless of which email client you use
 - NNTP, regardless of the email client
 - Regardless of the protocol (MAPI, HTTP) when using plug-ins for Microsoft Office Outlook and The Bat!
- Special plug-ins are available for the most common mail clients, such as Outlook, Microsoft Outlook Express, and The Bat!. These place email protection against both viruses directly in the mail client.
- The user notification function (see 14.11.1 on pg.180) has been expanded for certain protection events. You can select the method of notification by choosing from emails, sound notifications, popup messages, and logging the event.
- The program now has the ability to scan traffic sent over SSL protocol.
- The program has added self-defense features, including protection against unauthorized remote access of Anti-Virus services, and password protection for program settings. These features help keep malicious programs, hackers, and unauthorized users from disabling protection.
- The option of creating a rescue disk has been added. Using this disk, you can restart your operating system after a virus attack and scan it for malicious objects.

New Program Interface Features

- The new Kaspersky Anti-Virus interface makes the program's functions clear and easy to use. You can also change the program's appearance by using your own graphics and color schemes.
- The program regularly provides you with tips as you use it: Kaspersky Anti-Virus displays informative messages on the level of protection,

accompanies its operation with hints and tips, and includes a thorough Help section.

New Program Update Features

- This version of the application debuts our improved update procedure: Kaspersky Anti-Virus automatically checks the update source for update packages. When the program detects fresh updates, it downloads them and installs them on the computer.
- The program downloads updates incrementally, ignoring files that have already been downloaded. This lowers the download traffic for updates by up to 90%.
- Updates are downloaded from the fastest source.
- You can choose not to use a proxy server, by downloading program updates from a local source. This noticeably reduces the traffic on the proxy server.
- The program has an update rollback feature that can return to the previous version of the signatures, if, for example, the threat signatures are damaged or there is an error in copying.
- A feature has been added for distributing updates to a local folder to give other network computers access to them to save bandwidth.

2.2. The elements of Kaspersky Anti-Virus Defense

Kaspersky Anti-Virus protection is designed with the sources of threats in mind. In other words, a separate program component deals with each threat, monitoring it and taking the necessary action to prevent malicious effects of that threat on the user's data. This makes the system flexible, with user-friendly options for each of the components to fit the needs of a specific user or a business as a whole.

Kaspersky Anti-Virus includes:

- Protection Components (see 2.2.1 on pg. 22) that comprehensively defend all channels of data transmission and exchange on your computer.
- Virus Scan Tasks (see 2.2.2 on pg. 23) that virus-check the computer's memory and file system, as individual files, folders, disks, or regions.
- Support Tools (see 2.2.3 on pg. 23) that provide support for the program and extend its functionality.

2.2.1. Protection components

These protection components defend your computer in real time:

File Anti-Virus

A file system can contain viruses and other dangerous programs. Malicious programs can remain inactive in your file system for years after one day being copied from a floppy disk or from the Internet, without showing themselves at all. But you need only act upon the infected file, and the virus is instantly activated.

File Anti-virus is the component that monitors your computer's file system. It scans all files that can be opened, executed or saved on your computer and all connected disk drives. The program intercepts every attempt to access a file and scans the file for known viruses. If a file cannot be disinfected for any reason, it will be deleted, with a copy of the file either saved in Backup (see 14.2 on pg. 156), or moved to Quarantine (see 14.1 on pg. 153).

Mail Anti-Virus

Email is widely used by hackers to spread malicious programs, and is one of the most common methods of spreading worms. This makes it extremely important to monitor all email.

The *Mail Anti-Virus* component scans all incoming and outgoing email on your computer. It analyzes emails for malicious programs, only granting the addressee access to the email if it is free of dangerous objects.

Web Anti-Virus

By opening various web sites on the Internet, you risk infecting your computer with viruses that scripts on websites will install on your computer, and you risk downloading a dangerous object onto your computer.

Web Anti-Virus is specially designed to combat these risks, by intercepting and blocking scripts on web sites if they pose a threat, and by thoroughly monitoring all HTTP traffic.

Proactive Defense

With every new day, there are more and more malicious programs. They are becoming more complex, combining several types, and the methods they use to spread themselves are becoming harder and harder to detect.

To detect a new malicious program before it has time to do any damage, Kaspersky Lab has developed a special component, *Proactive Defense*. It is designed to monitor and analyze the behavior of all installed programs on your computer. Kaspersky Anti-Virus decides, based on the program's

actions: is it potentially dangerous? Proactive Defense protects your computer both from known viruses and from new ones that have yet to be discovered.

2.2.2. Virus scan tasks

In addition to constantly monitoring all potential pathways for malicious programs, it is extremely important to periodically scan your computer for viruses. This is necessary to detect malicious programs that were not previously discovered by the program because, for instance, its security level was set too low.

Kaspersky Anti-Virus configures, by default, three virus-scan tasks:

Critical Areas

Scans all critical areas of the computer for viruses. This includes: system memory, programs loaded on startup, boot sectors on the hard drive, and the *Windows* system directories. The task aims to detect active viruses quickly without fully scanning the computer.

My Computer

Scans for viruses on your computer with a thorough inspection of all disk drives, memory, and files.

Startup Objects

Scans for viruses in all programs that are loaded automatically on startup, plus RAM and boot sectors on hard drives.

There is also the option to create other virus-scan tasks and create a schedule for them. For example, you can create a scan task for email databases once per week, or a virus scan task for the **My Documents** folder.

2.2.3. Program tools

Kaspersky Anti-Virus includes a number of support tools, which are designed to provide real-time software support, expanding the capabilities of the program and assisting you as you go.

Updater

In order to be prepared for a hacker attack, or to delete a virus or some other dangerous program, Kaspersky Anti-Virus needs to be kept up-to-date. The *Updater* component is designed to do exactly that. It is responsible for updating the Kaspersky Anti-Virus threat signatures and internal modules.

The Update Distribution feature enables you to save updates for the threat signature and network drivers database, as well as application

modules retrieved from Kaspersky Lab servers, and then give other computers access to them to save bandwidth.

Data Files

Each security component, virus search task, and program update creates a report as it runs. The reports contain information on executed operations and their results. By using the *Reports* feature, you will remain up-to-date on the operation of all Kaspersky Anti-Virus components. Should problems arise, the reports can be sent to Kaspersky Lab, allowing our specialists to study the situation in greater depth and help you as quickly as possible.

Kaspersky Anti-Virus sends all files suspected of being dangerous to a special *Quarantine* area, where they are stored in encrypted form to avoid infecting the computer. You can scan these objects for viruses, restore them to their previous locations, delete them, or manually add files to Quarantine. Files that are found not to be infected upon completion of the virus scan are automatically restored to their former locations.

The *Backup* area holds copies of files disinfected and deleted by the program. These copies are created in case you either need to restore the files, or want information about their infection. These backup copies are also stored in an encrypted form to avoid further infection.

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

Rescue Disk

Kaspersky Anti-Virus can create a Rescue Disk, which provides a backup plan if system files are damaged by a virus attack and it is impossible to boot the operating system. By using the Rescue Disk in such a case, you can boot your computer and restore the system to the condition prior to the malicious action.

Support

All registered Kaspersky Anti-Virus users have access to our Technical Support team. To find out where you can receive technical support, use the *Support* feature.

Using the links, you can go to the Kaspersky Lab users forum and browse frequently asked questions with answers that might help you solve your problem. You can also send an error report or question on program operation to Technical Support by completing an on-line form.

You will also be able to access Technical Support on-line, and, of course, our employees will always be ready to assist you with Kaspersky Anti-Virus by phone.

2.3. Hardware and software system requirements

For Kaspersky Anti-Virus 6.0 to run properly, your computer must meet these minimum requirements:

General Requirements:

- 50 MB of free hard drive space
- CD-ROM drive (for installing Kaspersky Anti-Virus 6.0 from an installation CD)
- Microsoft Internet Explorer 5.5 or higher (for updating threat signatures and program modules through the Internet)
- Microsoft Windows Installer 2.0

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

- Intel Pentium 300 MHz processor or faster (or compatible).
- 64 MB of RAM

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a), Microsoft Windows 2000 Professional (Service Pack 2 or higher), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 or higher), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300 MHz processor or faster (or compatible).
- 128 MB of RAM.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) faster (or compatible).
- 512 MB of RAM.

2.4. Software packages

You can purchase the boxed version of Kaspersky Anti-Virus from our resellers, or download it from Internet shops, including the **eStore** section of www.kaspersky.com.

If you buy the boxed version of the program, the package will include:

- A sealed envelope with an installation CD containing the program files
- A User Guide
- The program activation code, attached to the installation CD envelope
- The end-user license agreement (EULA)

Before breaking the seal on the installation disk envelope, carefully read through the EULA.

If you buy Kaspersky Anti-Virus from an online store, you copy the product from the Kaspersky Lab website (**Downloads** → **Product Downloads**). You can download the User Guide from the **Downloads** → **Documentation** section.

You will be sent an activation code by email after your payment has been received.

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

Read the EULA through carefully.

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

By opening the sealed installation disk, you accept all the terms of the EULA.

2.5. Support for registered users

Kaspersky Lab provides its registered users with an array of services to make Kaspersky Anti-Virus more effective.

When the program has been activated, you become a registered user and will have the following services available until the license expires:

- New versions of the program free of charge
- Consultation on questions regarding installation, configuration, and operation of the program, by phone and email
- Notifications on new Kaspersky Lab product releases and new viruses (this services is for users that subscribe to Kaspersky Lab news mailings)

Kaspersky Lab does not provide technical support for operating system use and operation, or for any products other than its own.

CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS 6.0

You can fully or partially install Kaspersky Anti-Virus on your computer.

If you choose partial installation, you can select the components to install or automatically install just anti-virus components (see Step 9 of the installation procedure). You can install the other program components later, although you will need your installation disk to do so. You are advised to copy the installation disk to your hard drive.

You can install the application in the following ways:

- Using the installation wizard (see 3.1 on pg. 27)
- From the command prompt (see 3.3 on pg. 36)

3.1. Installation procedure using the Installation Wizard

Before beginning Kaspersky Anti-Virus installation, we recommend closing all other applications.

To install Kaspersky Anti-Virus on your computer, open the Windows Installer file on the installation CD.

Note:

Installing the program with an installer package downloaded from the Internet is identical to installing it from an installation CD.

An installation wizard will open for the program. Each window contains a set of buttons for navigating through the installation process. Here is a brief explanation of their functions:

- **Next** – accepts an action and moves forward to the next step of installation.
- **Back** – goes back to the previous step of installation.
- **Cancel** – cancels product installation.

- **Finish** – completes the program installation procedure.

Let's take a closer look at the steps of the installation procedure.

Step 1. Checking for the necessary system conditions to install Kaspersky Anti-Virus

Before the program is installed on your computer, the installer checks your computer for the operating system and service packs necessary to install Kaspersky Anti-Virus. It also checks your computer for other necessary programs and verifies that your user rights allow you to install software.

If any of these requirements is not met, the program will display a message informing you of the fault. You are advised to install any necessary service packs through **Windows Update**, and any other necessary programs, before installing Kaspersky Anti-Virus.

Step 2. Installation Welcome window

If your system fully meets all requirements, an installation window will appear when you open the installer file with information on beginning the installation of Kaspersky Anti-Virus.

To continue installation, click the **Next** button. You may cancel installation by clicking **Cancel**.

Step 3. Viewing the End-User License Agreement

The next window contains the End-User License Agreement between you and Kaspersky Lab. Carefully read through it, and if you agree to all the terms of the agreement, select **I accept the terms of the License Agreement** and click the **Next** button. Installation will continue.

Step 4. Selecting an installation folder

The next stage of Kaspersky Anti-Virus installation determines where the program will be installed on your computer. The default path is: **<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0**.

You can specify a different folder by clicking the **Browse** button and selecting it in the folder selection window, or by entering the path to the folder in the field available.

Remember that if you enter the full installation folder name manually, it must not exceed 200 characters or contain special characters.

To continue installation, click the **Next** button.

Step 5. Selecting an installation type

In this stage, you select how much of the program you want to install on your computer. You have three options:

Complete. If you select this option, all Kaspersky Anti-Virus components will be installed.

Custom. If you select this option, you can select the program components that you want to install. For more, see Step 6.

To select a setup type, click the appropriate button.

Step 6. Selecting program components to install

You will only see this step if you select the **Custom** setup type.

If you selected Custom installation, you can select the components of Kaspersky Anti-Virus that you want to install. By default, all components are selected.

To select the components you want to install, left-click the icon alongside a component name and select **Will be installed on local hard drive** from the context menu. You will find more information on what protection a selected component provides, and how much disk space it requires for installation, in the lower part of the program installation window.

If you do not want to install a component, select **Entire feature will be unavailable** from the context menu. Remember that by choosing not to install a component you deprive yourself of protection against a wide range of dangerous programs.

After you have selected the components you want to install, click **Next**. To return the list to the default programs to be installed, click **Reset**.

Step 7. Searching for other anti-virus programs

In this stage, the installer searches for other anti-virus products installed on your computer, including Kaspersky Lab products, which could raise compatibility issues with Kaspersky Anti-Virus.

The installer will display on screen a list of any such programs it detects. The program will ask you if you want to uninstall them before continuing installation.

You can select manual or automatic uninstall under the list of anti-virus applications detected.

If the list of anti-virus programs contains Kaspersky Anti-Virus® Personal or Kaspersky Anti-Virus® Personal Pro, we recommend saving the license key that

they use before deleting them, as you can use it as your license key for Kaspersky Anti-Virus 6.0. We also recommend saving Quarantine and Backup objects. These objects will automatically be moved to the Kaspersky Anti-Virus Quarantine and Backup and you can continue working with them.

To continue installation, click the **Next** button.

Step 8. Finishing installing your program

In this stage, the program will ask you to finish installing the program on your computer. You can decide if you want to use the protection settings, threat signatures from a previous version of Kaspersky Anti-Virus (for example, if you installed the beta version and now you are installing the commercial version).

Let's take a closer look at how to use the options described above.

If you have previously installed another version or build of Kaspersky Anti-Virus on your computer and you saved its threat signatures when you uninstalled it, you can use it in the current version. To do so, check **Threat signatures**. The threat signatures included with the program installation will not be copied to your computer.

To use protection settings that you configured and saved from a previous version, check **Protection settings**.

We do not recommend deselecting the **Enable Self-Defense before installation** when initially installing Kaspersky Anti-Virus 6.0. By enabling the protection modules, you can correctly roll back installation if errors occur while installing the program. If you are reinstalling the program, we recommend that you deselect this checkbox.

If the application is installed remotely via **Windows Remote Desktop**, we recommend checking **Enable Self-Defense before installation**. Otherwise the installation procedure might not complete or complete correctly.

To continue installation, click the **Next** button.

Step 9. Reading important information about the program

In this stage, the installer asks if you want to review important information about the program before getting started with Kaspersky Anti-Virus. This dialog box contains the basic features of Kaspersky Anti-Virus, with some facts about how it works.

To go on to the next step, click the **Next** button.

Step 10. Completing the installation procedure

The **Complete Installation** window contains information on finishing the Kaspersky Anti-Virus installation process.

If installation is completed successfully, a message on the screen will advise you to restart your computer. After restarting your system, the Kaspersky Anti-Virus Setup Wizard will automatically launch.

If there is no need for restarting your system to complete the installation, click **Next** to go on to the Setup Wizard.

3.2. Setup Wizard

The Kaspersky Anti-Virus 6.0 Setup Wizard starts after the program has finished installation. It is designed to help you configure the initial program settings to conform to the features and uses of your computer.

The Setup Wizard interface is designed like a standard Windows Wizard and consists of a series of steps that you can move between using the **Back** and **Next** buttons, or complete using the **Finished** button. The **Cancel** button will stop the Wizard at any point.

You can skip this initial settings stage when installing the program by closing the Wizard window. In the future, you can run it again from the program interface if you restore the default settings for Kaspersky Anti-Virus (see 6.6 on page 71).

3.2.1. Using objects saved with Version 5.0

This wizard window appears when you install the application on top of Kaspersky Anti-Virus 5.0. You will be asked to select what data used by version 5.0 you want to import to version 6.0. This might include quarantined or backup files or protection settings.

To use this data in Version 6.0, check the necessary boxes.

3.2.2. Activating the program

You can activate the program by installing a license key. Kaspersky Anti-Virus check for a license agreement and to determine its expiration date.

The license key contains system information necessary for all the program's features to operate, and other information:

- Support information (who provides program support and where you can obtain it)
- Name, number, and expiration date of your license

Warning!

You must have an Internet connection to activate the program. If you are not connected to the Internet during installation, you can activate the program later from the program interface (see 14.5 on pg. 168).

3.2.2.1. Selecting a program activation method

There are several options for activating the program, depending on whether you have a license key for Kaspersky Anti-Virus or need to obtain one from the Kaspersky Lab server:

- ① **Activate using the activation code.** Select this activation option if you have purchased the full version of the program and were provided with an activation code. Using this code, you will receive a license key that provides you with complete access to all the program's features until the license expires.
- ② **Activate trial version.** Select this activation option if you want to install a trial version of the program before making the decision to purchase the commercial version. You will be provided with a free license key with a limited trial period.
- ③ **Apply existing license key.** Activate the application using the license key file for Kaspersky Anti-Virus 6.0 obtained earlier.
- ④ **Activate later.** If you choose this option, you will skip the activation stage. Kaspersky Anti-Virus 6.0 will be installed on your computer and you will have access to all program features except updates (you can only update the threat signatures once after installing the program).

The first two activation options use a Kaspersky Lab web server, which requires an Internet connection. Before activating, make sure to edit your network settings (see 13.4.3 on pg. 147) in the window that opens when you click **LAN Settings** if necessary. For more in-depth information on configuring network settings, contact your system administrator or ISP.

3.2.2.2. Entering the activation code

To activate the program, you must enter the activation code that was provided when you purchased the program. The activation code must be entered in Latin letters.

Enter your personal information in the lower part of the window: full name, email address, and country and city of residence. This information might be requested to identify a registered user if a key is lost or stolen. If this happens, you can obtain a new license key with the personal information.

3.2.2.3. Obtaining a license key

The Setup Wizard connects to Kaspersky Lab servers and sends them your registration data (the activation code and personal information) for inspection.

If the activation code passes inspection, the Wizard receives a license key file. If you install the demo version of the program, the Setup Wizard will receive a trial key file without an activation code.

The file received will be installed automatically and you will see an activation completion window with detailed information on the license.

If the activation code does not pass inspection, an information message will be displayed on the screen. If this occurs, contact the software vendors from whom you purchased the program for more information.

3.2.2.4. Selecting a license key file

If you have a license key file for Kaspersky Anti-Virus 6.0, the Wizard will ask if you want to install it. If you do, use the **Browse** button and select the file path for the key file with the *.key* extension in the file selection window.

After you have successfully installed the key, you will see information about the license in the lower part of the window: name of the person to whom the software is registered, license number, license type (full, beta-testing, demo, etc.), and the expiration date for the license.

3.2.2.5. Completing program activation

The Setup Wizard will inform you that the program has been successfully activated. It will also display information on the license key installed: name of the person to whom the software is registered, license number, license type (full, beta-testing, demo, etc.), and the expiration date for the license.

3.2.3. Selecting a security mode

In this window, the Settings Wizard asks you to select the security mode that the program will operated with:

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

Interactive. This mode provides more customized defense of your computer's data than Basic mode. It can trace attempts to alter system settings and suspicious activity in the system.

All of the activities listed above could be signs of malicious programs or standard activity for some of the programs you use on your computer. You will have to decide for each separate case whether those activities should be allowed or blocked.

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

- Enable Registry Guard** – ask for user decision if attempts to alter system registry keys are detected.

If the application is installed on a computer running Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64, the interactive mode settings listed below will not be available.

- Enable Application Integrity Control** – prompt user to confirm actions taken when modules are loaded into applications being monitored.
- Enable Extended Proactive Defense** – enable analysis of all suspicious activity in the system, including opening browser with command line settings, loading into program processes, and window hooks (these settings are disabled by default).

3.2.4. Configuring update settings

Your computer's security depends directly on updating the threat signatures and program modules regularly. In this window, the Setup Wizard asks you to select a mode for program updates, and to configure a schedule.

- Automatically.** Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scans can be set to be more frequent during virus outbreaks and less so when they are over. When the program detects fresh updates, it downloads them and installs them on the computer. This is the default setting.
- Every 1 day(s).** Updates will run automatically according to the schedule created. You can configure the schedule by clicking **Change**.
- Manually.** If you choose this option, you will run program updates yourself.

Note that the threat signatures and program modules included with the software may be outdated by the time you install the program. That is why we recommend downloading the latest program updates. To do so, click **Update now**. Then Kaspersky Anti-Virus will download the necessary updates from the update servers and will install them on your computer.

If you want to configure updates (set up network properties, select the resource from which updates will be downloaded, or select the update server located nearest to you), click **Settings**.

3.2.5. Configuring a virus scan schedule

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

When you install Kaspersky Anti-Virus, three default virus scan tasks are created. In this window, the Settings Master asks you to choose a scan task setting:

Scan startup objects

Kaspersky Anti-Virus scans startup objects automatically when it is started by default. You can edit the schedule settings in another window by clicking **Change**.

Scan critical areas

To automatically scan critical areas of your computer (system memory, Startup objects, boot sectors, Windows system folders) for viruses, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting for this automatic scan is disabled.

Full computer scan

For a full virus scan of your computer to run automatically, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting, for scheduled running of this task, is disabled. However, we recommend running a full virus scan of your computer immediately after installing the program.

3.2.6. Restricting program access

Since several people with different levels of computer literacy might use a personal computer, and since malicious programs can disable protection, you are given the option of password-protecting access to Kaspersky Anti-Virus. Using a password can protect the program from unauthorized attempts to disable protecting or change settings.

To enable password protection, check **Enable password protection** and complete the **Password** and **Confirm password** fields.

Select the area below that you want password protection to apply to:

- All operations (except notifications of dangerous events).** Request password if the user attempts any action with the program, except for responses to notifications on detection of dangerous objects.
- Selected operations:**
 - Saving program settings** – request password when a user attempts to save changes to program settings.
 - Exiting the program** – request password if a user attempts to close the program.
 - Stopping/pausing protection components or virus scan tasks** – request password if user attempts to pause or fully disable any protection component or virus scan task.

3.2.7. Application Integrity Control

In this stage, the Kaspersky Anti-Virus wizard will analyze the applications installed on your computer (dynamic library files, digital manufacture signatures), count application checksum files, and create a list of programs that can be trusted from a virus security perspective. For example, this list will automatically include all applications digitally signed by Microsoft.

In the future, Kaspersky Anti-Virus will use information obtained while analyzing application structure to prevent malicious code from being imbedded in application modules.

Analyzing the applications installed on your computer may take some time.

3.2.8. Finishing the Setup Wizard

The last window of the Wizard will ask if you want to restart your computer to complete the program installation. You must restart for some of the Kaspersky Anti-Virus component drivers to register correctly.

You can wait to restart, but if you do, some program components will not work.

3.3. Installing the program from the command prompt

To install Kaspersky Anti-Virus 6.0, enter this at the command prompt:

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

The Installation Wizard will start (see 3.1 on pg. 27). Once the program is installed, you must restart the computer.

You can also use one of the following methods when installing the application.

To install the application in the background without restarting the computer (the computer should be restarted manually after installation), enter :

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

To install the application in the background and then restart the computer, enter:

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

3.4. Upgrading from 5.0 to 6.0

If Kaspersky Anti-Virus 5.0 Personal or Kaspersky Anti-Virus 5.0 Personal Pro is installed on your computer, you can upgrade it to Kaspersky Anti-Virus 6.0.

After you start the Kaspersky Anti-Virus 6.0 installation program, you will be given the choice of first uninstalling the already installed version 5.0. Once the uninstall process is complete, you must restart your computer, after which version 6.0 installation will run 6.0.

Warning!

When you upgrade Kaspersky Anti-Virus 5.0 to 6.0 from a password-protected network folder, version 5.0 will be uninstalled and the computer will be restarted without then installing version 6.0 of the application. This is because the installer program does not have access privileges to the network folder. To resolve this problem, only run the installer from a local folder.

CHAPTER 4. PROGRAM INTERFACE

Kaspersky Anti-Virus has a straightforward, user-friendly interface. This chapter will discuss its basic features:

- System tray icon (see 4.1 on pg. 38)
- Context menu (see 4.2 on pg. 39)
- Main window (see 4.3 on pg. 40)
- Program settings window (see 4.4 on pg. 43)

In addition to the main program interface, there are plug-ins for the following applications:



- Microsoft Office Outlook;
- The Bat!;
- Microsoft Windows Explorer.

The plug-ins extend the functionality of these programs by making Kaspersky Anti-Virus management and settings possible from their interfaces.

4.1. System tray icon

As soon as you install Kaspersky Anti-Virus, its icon will appear in the system tray.





The icon is an indicator for Kaspersky Anti-Virus functions. It reflects the state of protection and shows a number of basic functions performed by the program.

If the icon is active  (color), this means that your computer is being protected. If the icon is inactive  (black and white), this means that protection is either fully stopped or that some protection components (see 2.2.1 on pg. 22) are paused.

The Kaspersky Anti-Virus icon changes in relation to the operation being performed:



Emails are being scanned.

-  Scripts are being scanned.
-  A file that you or some program is opening, saving, or running is being scanned.
-  Kaspersky Anti-Virus threat signatures and program modules are being updated.
-  An error has occurred in some Kaspersky Anti-Virus component.

The icon also provides access to the basics of the program interface: the context menu (see 4.2 on pg. 39) and the main window (see 4.3 on pg. 40).

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

To open the Kaspersky Anti-Virus main window at the **Protection** section (this is the default first screen when you open the program), double-click the program icon. If you single-click the icon, the main window will open at the section that was active when you last closed it.

4.2. The context menu

You can perform basic protection tasks from the context menu (see fig. 1).



Figure 1. The context menu

The Kaspersky Anti-Virus menu contains the following items:

- Scan My Computer** – launches a complete scan of your computer for dangerous objects. The files on all drives, including removable storage media, will be scanned.
- Virus scan...** – selects objects and starts scanning them for viruses. The default list contains a number of files, such as the **My Documents** folder, the Startup folder, email databases, all the drives on your

computer, etc. You can add to the list, select files to be scanned, and start virus scans.

Update – download updates to program modules and threat signatures and install them on your computer.

Activate... – activate the program. This menu item is only available if the program is not activated.

Settings... – view and configure settings for Kaspersky Anti-Virus.

Open Kaspersky Anti-Virus – open the main program window (see 4.3 on pg. 40).

Pause Protection / Resume Protection – temporarily disable or enable protection components (see 2.2.1 on pg. 22). This menu item does not affect program updates or virus scan tasks.

Exit – close Kaspersky Anti-Virus.

If a virus search task is running, the context menu will display its name with a percentage progress meter. By selecting the task, you can open the report window to view current performance results.

4.3. Main program window

The Kaspersky Anti-Virus main window (see fig. 2) provides you with a straightforward, user-friendly interface to manage the program. It can be divided into two parts:

- the left part of the window, the navigation panel, guides you quickly and easily to any component, virus scan task performance, or the program's support tools;
- the right part of the window, the information panel, contains information on the protection component selected in the left part of the window and displays settings for each of them, giving you tools to carry out virus scans, work with quarantined files and backup copies, manage license keys, and so on.

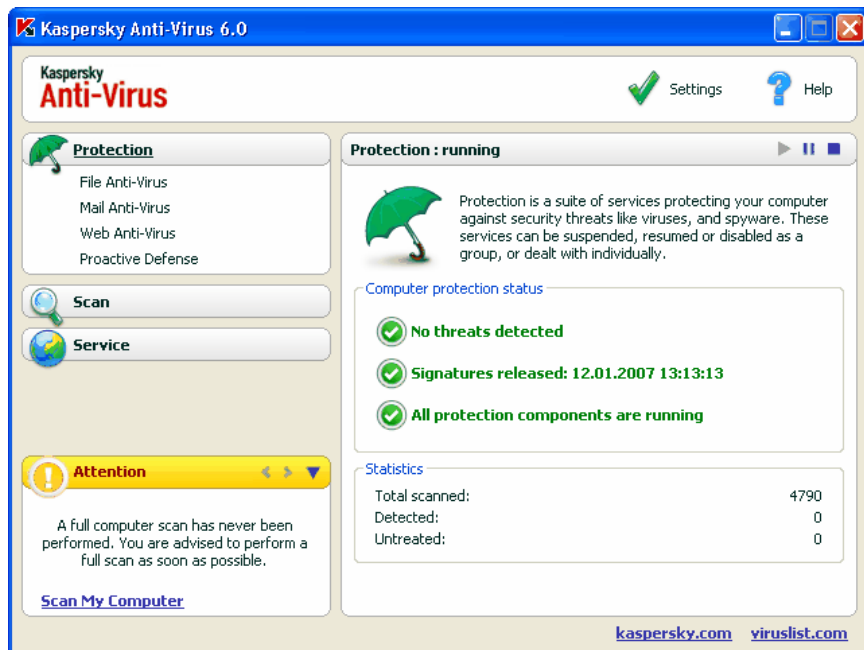

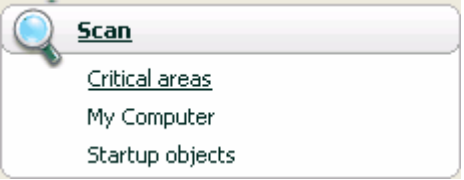


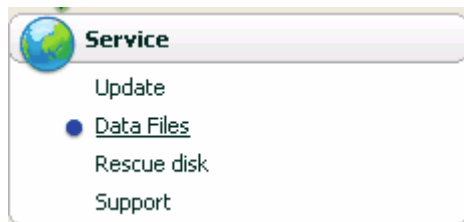
Figure 2. Kaspersky Anti-Virus main window

After selecting a section or component in the left part of the window, you will find information in the right-hand part that matches your selection.

We will now examine the elements in the main window's navigation panel in greater detail.

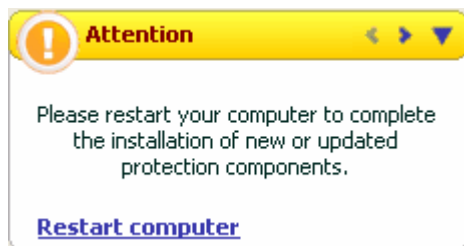
| Main Window Section | Purpose |
|--|--|
| <p>This window mostly informs you of the protection status of your computer. The Protection section is designed for exactly that.</p>  | <p>Here you will find general information about Kaspersky Anti-Virus operations, allowing you to verify that all the components are running correctly and examine the general statistics.</p> <p>You can also enable/disable protection components here.</p> <p>To view statistics and settings for a specific protection component, you need only select the name of the component about which you want information in the Protection section.</p> |
| <p>To scan your computer for malicious files or programs, use the special Scan section in the main window.</p>  | <p>This section contains a list of objects that can be scanned for viruses.</p> <p>You can also create virus scan tasks in this section that will be displayed in the navigation panel. This feature makes launching virus scans noticeably easier.</p> <p>The commonest and most important tasks are included in the section. These include virus scan tasks for critical areas, for startup programs, and a full computer scan.</p> |

The **Service** section includes additional Kaspersky Anti-Virus features.



Here you can update the program, view [reports](#) on the performance of any of the Kaspersky Anti-Virus components, work with [quarantined objects](#) and [backup copies](#), review [technical support information](#), create a [Rescue Disk](#) and [manage license keys](#).

The **Comments and tips** section accompanies you as you use the application.



This section offers tips on raising the security level of your computer. You will also find comments on the application's current performance and its settings. The links in this section guide you to take the actions recommended for a particular section or to view information in more detail.

Each element of the navigation panel is accompanied by a special context menu. The menu contains points for the protection components and tools that help the user quickly configure them, manage them, and view reports. There is an additional menu item for virus scan and update tasks that allows you to create your own task, by modifying a copy of an existing task.

You can change the appearance of the program by creating and using your own graphics and color schemes.

4.4. Program settings window

You can open the Kaspersky Anti-Virus settings window from the main window (see 4.3 on pg. 40). To do so, click [Settings](#) in the upper part of it.

The settings window (see fig. 3) is similar in layout to the main window:

- the left part of the window gives you quick and easy access to the settings for each of the program components, virus search tasks, and program tools;

- the right part of the window contains a detailed list of settings for the item selected in the left part of the window.

When you select any section, component, or task in the left part of the settings window, the right part will display its basic settings. To configure advanced settings, you can open second and third level settings windows by clicking on the corresponding buttons. You can find a detailed description of program settings in the appropriate sections of the user guide.

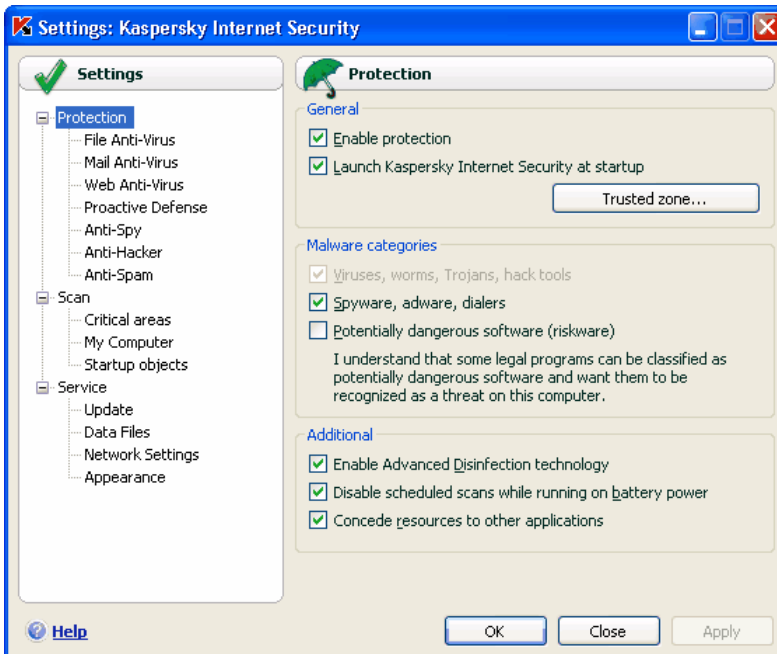


Figure 3. Kaspersky Anti-Virus settings window

CHAPTER 5. GETTING STARTED

One of Kaspersky Lab's main goals in creating Kaspersky Anti-Virus was to provide optimum configuration for each of the program's options. This makes it possible for a user with any level of computer literacy to quickly protect their computer straight after installation.

However, configuration details for your computer, or the jobs you use it for, can have their own specific requirements. That is why we recommend performing a preliminary configuration to achieve the most flexible, personalized protection of your computer.

To make getting started easier, we have combined all the preliminary configuration stages in one Setup Wizard (see 3.2 on pg. 31) that starts as soon as the program is installed. By following the Wizard's instructions, you can activate the program, configure settings for updates and virus scans, password-protect access to the program.

After installing and starting the program, we recommend that you take the following steps:

- Check the current protection status (see 5.1 on pg. 45) to make sure that Kaspersky Anti-Virus is running at the appropriate level.
- Update the program (see 5.5 on pg. 52) if the Settings Wizard did not do so automatically after installing the program.
- Scan the computer (see 5.2 on pg. 50) for viruses.

5.1. What is the protection status of my computer?

Composite information on your computer's protection is provided in the main program window, in the **Protection** section. The *current protection status* of the computer and the *general performance statistics* of the program are displayed here.

Computer protection status displays the current state of protection for your computer using special indicators (see 5.1.1 on pg. 46). **Statistics** (see 5.1.2 on pg. 49) analyses the current program session.

5.1.1. Protection indicators

Protection status is determined by three indicators, each of which reflect a different aspect of your computer's protection at any given moment, and indicate any problems in program settings and performance.

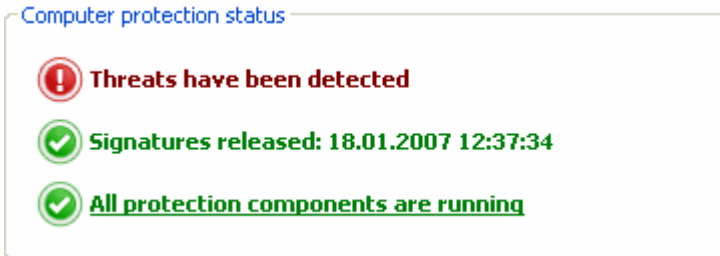


Figure 4. Indicators reflecting the computer protection status

Each indicator has three possible appearances:



– *the situation is normal*; the indicator is showing that your computer's protection is adequate, and that there are no problems in the program settings or performance.



– *there are one or more deviations* in Kaspersky Anti-Virus performance from the recommended level of performance, which could affect information security. Please pay heed to the actions recommended by Kaspersky Lab, which are given as links.



– *the computer's security status is critical*. Please follow the recommendations closely to improve your computer's protection. The recommended actions are given as links.

We will now examine protection indicators and the situations that each of them indicate in more detail.

The first indicator reflects the situation with malicious files and programs on your computer. The three values of this indicator mean the following:



No threats detected

Kaspersky Anti-Virus has not detected any dangerous files or programs on your computer.

All threats have been neutralized

Kaspersky Anti-Virus has treated all infected files and programs, and deleted those that could not be treated.



Hacker attack has been blocked

Kaspersky Anti-Virus has detected and blocked an attempted network attack.



Threats have been detected

Your computer is at risk of infection. Kaspersky Anti-Virus has detected malicious programs (viruses, Trojans, worms, etc.) that must be neutralized. To do so, use the [Neutralize all](#) link. Click the [Details](#) link to see more detailed information about the malicious objects.

Please restart your computer

In order to process the malicious files or programs, you must restart your computer. Save and close all files that you are working with and use the [Restart computer](#) link.

The [second indicator](#) shows the effectiveness of your computer's protection. The indicator takes one of the following values:



Signatures released: (date, time)

Both the application and the threat signatures used by Kaspersky Anti-Virus are most recent versions.



Signatures are out of date

The Kaspersky Anti-Virus internal modules and threat signatures have not been updated for several days. You are running the risk of infecting your computer with new malicious programs that have appeared since you last updated the program. We recommend updating Kaspersky Anti-Virus. To do so, use the [Update](#) link.

Please restart your computer

You must restart your system for the program to run correctly. Save and close all files that you are working with and use the [Restart computer](#) link.



Signatures are obsolete

Kaspersky Anti-Virus has not been updated for some time. You are putting the data at great risk. Update the program as

soon as possible. To do so, use the [Update](#) link..

Signatures are corrupted or partially corrupted

The threat signature files are fully or partially damaged. If this occurs, it is recommended to run program updates again. If you encounter the same error message again, contact the Kaspersky Lab Technical Support Service.

The third indicator shows the current functionality of the program. The indicator takes one of the following values:



All protection components are running

Kaspersky Anti-Virus is protecting your computer on all channels by which malicious programs could penetrate. All protective components are enabled.

Protection is not installed

When Kaspersky Anti-Virus was installed, none of the monitoring components were installed. This means you can only scan for viruses. For maximum security, you should install protection components on your computer.



Some protection components are paused

One or more protection components has been paused. In order to restore the inactive component, select it from the list and click ►.

All protection components are paused

All protection components have been paused. To restore the components, select **Resume protection** from the context menu by clicking on the system tray icon.

Some protection components are disabled

One or several protection components is stopped. This could lead to your computer becoming infected and losing data. You are strongly advised to enable protection. To do so, select an inactive component from the list and click ►.

All protection components are disabled

Protection is fully disabled. No components are running. To restore the components, select **Resume protection** from the context menu by clicking on the system tray icon.



Some protection components have malfunctioned

One or more Kaspersky Anti-Virus components has internal errors. If this occurs, you are advised to enable the component or restart the computer, as it is possible that the component drivers have to be registered after being updated.

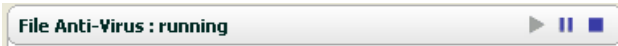
5.1.2. Kaspersky Anti-Virus component status

To determine how Kaspersky Anti-Virus is guarding your file system, email, HTTP traffic, or other areas where dangerous programs could penetrate your computer, or to view the progress of a virus scan task or threat signature update, simply open the corresponding section of the main program window.

For example, to view the current File Anti-Virus status, select **File Anti-Virus** from the left-hand panel of the main window, or to see if you are being protected against new viruses, select **Proactive Defense**. The right-hand panel will display a summary of information about the component's operation.

For protection components, the right-hand panel contains the **status bar**, the **Status** box and the **Statistics** box.

For the File Anti-Virus component, the *status bar* appears as follows:



- *File Anti-Virus : running* – file protection is active for the level selected (see 7.1 on pg. 73).
- *File Anti-Virus : paused* – File Anti-Virus is disabled for a set period of time. The component will resume operation automatically after the assigned period has expired or after the program is restarted. You can also resume file protection manually, by clicking the ► button located on the status bar.
- *File Anti-Virus : stopped* – the component has been stopped by the user. You can resume file protection manually, by clicking the ► button located on the status bar.
- *File Anti-Virus : not running* – file protection is not available for some reason. For example, you do not have a license key for the program.
- *File Anti-Virus : disabled (error)* – the component encountered an error. If this occurs, contact Kaspersky Lab's Technical Support.

If the component contains several modules, the **Status** section will contain information on the status of each of them. For components that do not have

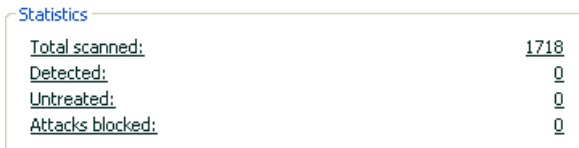
individual modules, their status, security level, and, for some components, the response to dangerous programs are displayed.

There is no **Status** box for virus scan and update tasks. The security level, the action applied to dangerous programs for virus scan tasks, and the run mode for updates are listed in the **Settings** box.

The **Statistics** box contains information on the operation of protection components, updates, or virus scan tasks.

5.1.3. Program performance statistics

Program statistics can be found in the **Statistics** box of the main window's **Protection** section, and display general information on computer protection, recorded from the time that Kaspersky Anti-Virus was installed.



| Statistics | |
|------------------|------|
| Total scanned: | 1718 |
| Detected: | 0 |
| Untreated: | 0 |
| Attacks blocked: | 0 |

Figure 5. The program's general statistics box

You can left-click anywhere in the box to view a report with detailed information. The tabs display:

- Information on objects found (see 14.3.2 on pg. 161) and the status assigned to them
- Event log (see 14.3.3 on pg. 162)
- General scan statistics (see 14.3.4 on pg. 163) for your computer
- Program performance settings (see 14.3.5 on pg. 164)

5.2. How to scan your computer for viruses

After installation, the application will without fail inform you with a special notice in the lower left-hand part of the application window that the computer has not yet been scanned and will recommend that you scan it for viruses immediately.

Kaspersky Anti-Virus includes a task for a computer virus scan located in the **Scan** section of the program's main window.

After you select the task named **My Computer**, the right-hand panel will display the following: statistics for the most recent computer scan; task settings; what level of protection is selected, and what actions will be taken for dangerous objects.

To scan your computer for malicious programs,

Click the **Scan** button in the right-hand part of the screen.

As a result, the program will start scanning your computer, and the details will be shown in a special window. When you click the **Close** button, the window with information about installation progress will be hidden. This will not stop the scan.

5.3. How to scan critical areas of the computer

There are areas on your computer that are critical from a security perspective. These are targeted by malicious programs malicious programs aimed at damaging your operating system, processor, memory, etc.

It is extremely important to protect these critical areas so that your computer keeps running. There is a special virus scan task for these areas, which is located in the program's main window in the **Scan** section.

After selecting the task named **Critical areas**, the right-hand panel of the main window will display the following: statistics for the most recent scan of these areas; task settings; what level of protection was selected, and what actions are applied to security threats. Here you can also select which critical areas you want to scan, and immediately scan those areas.

To scan critical areas of your computer for malicious programs,

Click the **Scan** button in the right-hand part of the screen.

When you do this, a scan of the selected areas will begin, and the details will be shown in a special window. When you click the **Close** button, the window with information about installation progress will be hidden. This will not stop the scan.

5.4. How to scan a file, folder or disk for viruses

Sometimes it is necessary to scan individual objects for viruses but not the entire computer: for example, a portable hard drive or memory stick used to transfer files between the office and home computers. You can select an object for

scanning with the standard tools of the Windows operating system (for example, in the **Explorer** program window, on your **Desktop**, etc.).

To scan an object,

Place the cursor over the name of the selected object, open the Windows context menu by right-clicking, and select **Scan for Viruses** (see fig. 6).

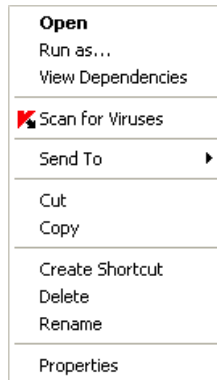


Figure 6. Scanning an object selected using a standard Windows context-sensitive menu

A scan of the selected object will then begin, and the details will be shown in a special window. When you click the **Close** button, the window with information about installation progress will be hidden. This will not stop the scan.

5.5. How to update the program

Kaspersky Lab updates the threats signatures and internal modules for Kaspersky Anti-Virus using dedicated update servers.

Kaspersky Lab's update servers are the Kaspersky Lab Internet sites where the program updates are stored.

Warning!

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

By default, Kaspersky Anti-Virus automatically checks for updates on the Kaspersky Lab servers. If the server has the latest updates, Kaspersky Anti-Virus will download and install them in silent mode.

To update Kaspersky Anti-Virus manually,

select the **Update** component in the **Service** section of the main program window and click the **Update now!** button in the right-hand part of the window.

As a result, Kaspersky Anti-Virus will begin the update process, and display the details of the process in a special window.

5.6. What to do if protection is not running

If problems or errors arise in the performance of any protection component, be sure to check its status. If the component status is *not running* or *operation error*, try restarting Kaspersky Anti-Virus.

If the problem is not resolved after you restart your computer, we recommend correctly possible errors using the application rollback program (see Chapter 16 on pg. 201).

If the application restore procedure does not help, contact Kaspersky Lab Technical Support. You may need to save a report on component operation or the entire application to file and send it to Technical Support for further study.

To save the report to file:

1. Select the component in the **Protection** section of the main window of the program and left-click anywhere in the **Statistics** box.
2. Click the **Save As** button and in the window that opens specify the file name for the component's performance report.

To save a report for all Kaspersky Anti-Virus components at once (protection components, virus scan tasks, support features):

1. Select the **Protection** section in the main window of the program and left-click anywhere in the **Statistics** box.

or

Click All reports in the report window for any component. Then the **Reports** tab will list reports for all program components.

2. Click the **Save As** button and in the window that opens specify a file name for the program's performance report.

CHAPTER 6. PROTECTION MANAGEMENT SYSTEM

Kaspersky Anti-Virus lets you multi-task computer security management:

- Enable, disable, and pause (see 6.1 on pg. 54) the program
- Define the types of dangerous programs (see 6.2 on pg. 58) against which Kaspersky Anti-Virus will protect your computer
- Create an exclusion list (see 6.3 on pg. 59) for protection
- Create your own virus scan and update tasks (see 6.4 on pg. 68)
- Configure a virus scan schedule (see 6.5 on pg. 69).
- Configure power settings for anti-virus protection (see 6.6 on pg. 71)

6.1. Stopping and resuming protection on your computer

By default, Kaspersky Anti-Virus boots at startup and protects your computer the entire time you are using it. The words *Kaspersky Anti-Virus 6.0* in the upper right-hand corner of the screen let you know this. All protection components (see 2.2 on pg. 21) are running.

You can fully or partially disable the protection provided by Kaspersky Anti-Virus.

Warning!

Kaspersky Lab strongly recommend that you **do not disable protection**, since this could lead to an infection on your computer and consequent data loss.

Note that in this case protection is discussed in the context of the protection components. Disabling or pausing protection components does not affect the performance of virus scan tasks or program updates.

6.1.1. Pausing protection

Pausing protection means temporarily disabling all the components that monitor the files on your computer, incoming and outgoing email, executable scripts, application behavior.

To pause a Kaspersky Anti-Virus operation:

1. Select **Pause protection** in the program's context menu (see 4.2 on pg. 39).
2. In the Pause Protection window that opens (see fig. 7), select how soon you want protection to resume:
 - **In <time interval>** – protection will be enabled after this amount of time. To select a time value, use the drop-down menu.
 - **At next program restart** – protection will resume if you open the program from the Start Menu or after you restart your computer (provided the program is set to start when the computer is turned on; see 6.1.5 on pg. 58).
 - **By user request only** – protection will stop until you start it yourself. To enable protection, select **Resume protection** from the program's context menu.

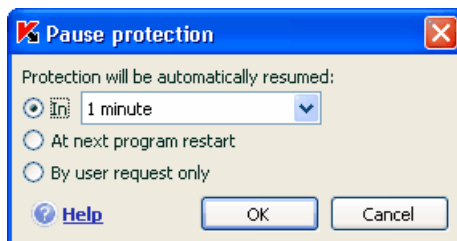


Figure 7. Pause protection window


Tip:

You can also stop protection on your computer with one of the following methods:

- Click the **||** button in the **Protection** section.
- Select **Exit** from the context menu.

If you pause protection, all protection components will be paused. This is indicated by:

- Inactive (gray) names of the disabled components in the Protection section of the main window.
- Inactive (gray) system tray icon.

- The third protection indicator (see 5.1.1 on pg. 46) on your computer, which shows that  **No protection components are enabled.**

6.1.2. Stopping protection


Stopping protection means fully disabling your protection components. Virus scans and updates continue to work in this mode.

If protection is stopped, it can be only be resumed by the user: protection components will not automatically resume after system or program restarts. Remember that if Kaspersky Anti-Virus is somehow in conflict with other programs installed on your computer, you can pause individual components or create an exclusion (see 6.3 on pg. 59) list.

To stop all protection:

1. Open the Kaspersky Anti-Virus main window.
2. Select the **Protection** section and click **Settings**.
3. In the program settings window, uncheck **Enable protection**.


After disabling protection, all protection components will stop. This is indicated by:


- Inactive (gray) names of the disabled components in the Protection section of the main window.
- Inactive (gray) system tray icon.
- The third protection indicator (see 5.1.1 on pg. 46) on your computer, which shows that  **All protection components are disabled.**

6.1.3. Pausing / stopping protection components, virus scans, and update tasks

There are several ways to stop a protection component, virus scan, or update. Before doing so, you are strongly advised to establish why you need to stop them. It is likely that the problem can be solved in another way, for example, by changing the security level. If, for example, you are working with a database that you are sure does not contain viruses, simply add its files as an exclusion (see 6.3 on pg. 59).



To pause protection components, virus scans, and update tasks:


Select the component or task from the left-hand part of the main window and click the  button on the status bar.

The component/task status will change to **paused**. The component or task will be paused until you resume it by clicking the  button.

When you pause the component or a task, statistics for the current Kaspersky Anti-Virus session are saved and will continue to be recorded after the component is updated.

To stop protection components, virus scans, and update tasks:

Click the  button on the status bar. You can also stop protection components in the program settings window by deselecting  **Enable <component name>** in the **General** section for that component.

The component/task status will then change to *stopped (disabled)*. The component or task will be stopped until you enable it by clicking the  button. For virus scan and update tasks, you will have the choice of the following options: continue the task that was interrupted, or restart it from the beginning.

When you stop a real-time protection component or a task, all the statistics from previous work are cleared and when the component is started they are recorded over.


6.1.4. Restoring protection on your computer

If at some point you paused or stopped protection on your computer, you can resume it using one of the following methods:

- *From the context menu.*

To do so, select **Resume protection**.

- *From the program's main window.*

To do so, click the  button on the status bar in the **Protection** section of the main window.

The protection status immediately changes to **running**. The program's system tray icon becomes active (color). The third protection indicator (see 5.1.1 on

pg. 46) will also inform you that  **All protection components are running**.

6.1.5. Shutting down the program

If you have to shut down Kaspersky Anti-Virus, select **Exit** from the program's context menu (see 4.2 on pg. 39). This will close the program, leaving your computer unprotected.

If network connections that the program monitors are active on your computer when you close the program, a notice will appear on the screen stating that these connections will be interrupted. This is necessary for the program to shut down correctly. The connections are terminated automatically after ten seconds or by clicking the **Yes** button. The majority of connections will resume automatically after a short while.

Note that if you are downloading a file without a download manager when the connection is terminated, the file transfer will be lost. You will have to download the file over again.

You can choose not to interrupt the connections by clicking on the **No** button in the notice window. If you do so, the program will continue running.

After closing the program, you can enable computer protection again by opening Kaspersky Anti-Virus (**Start** → **Programs** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**).

You can also resume protection automatically after restarting your operating system. To enable this feature, select the **Protection** section in the program settings window and check **Launch Kaspersky Anti-Virus at startup**.

6.2. Types of programs to be monitored

Kaspersky Anti-Virus protects you from various types of malicious programs. Regardless of your settings, the program always scans and neutralizes viruses, Trojans, and hack tools. These programs can do the significant damage to your computer. To make your computer more secure, you can expand the list of threats that the program will detect by making it monitor additional types of dangerous programs.

To choose what malicious programs Kaspersky Anti-Virus will protect you from, select the **Protection** section in the program settings window (see 4.4 on pg. 43).

The **Malware categories** box contains threat types:

- Viruses, worms, Trojans, hack tools.** This group combines the most common and dangerous categories of malicious programs. This is the

minimum admissible security level. Per recommendations of Kaspersky Lab experts, Kaspersky Anti-Virus always monitors this category of malicious programs.

- ✔ **Spyware, adware, dialers.** This group includes potentially dangerous software that may inconvenience the user or incur serious damage.
- ✔ **Potentially dangerous software (riskware).** This group includes programs that are not malicious or dangerous. However, under certain circumstances they could be used to cause harm to your computer.

The groups listed above comprise the full range of threats which the program detects when scanning objects.

If all groups are selected, Kaspersky Anti-Virus provides the fullest possible anti-virus protection for your computer. If the second and third groups are disabled, the program will only protect you from the commonest malicious programs.

Kaspersky Lab does not recommend disabling monitoring for the second group. If a situation arises when Kaspersky Anti-Virus classifies a program that you do not consider dangerous as a potentially dangerous program, we recommend creating an exclusion for it (see 6.3 on pg. 59).

6.3. Creating a trusted zone

A *trusted zone* is a list of objects created by the user, that Kaspersky Anti-Virus does not monitor. In other words, it is a set of programs excluded from protection.

The user creates a protected zone based on the properties of the files she uses and the programs installed on his computer. You might need to create such an exclusion list if, for example, Kaspersky Anti-Virus blocks access to an object or program and you are sure that the file or program is absolutely safe.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area (for example, a folder or a program), program processes, or objects according to Virus Encyclopedia classification (the status that the program assigns to objects during a scan).

Warning!

Excluded objects are not subject to scans when the disk or folder where they are located are scanned. However, if you select that object in particular, the exclusion rule will not apply.

In order to create an exclusion list,

1. Open the Kaspersky Anti-Virus settings window and select the **Protection** section.

2. Click the **Trusted zone** button in the **General** section.
3. Configure exclusion rules for objects and create a list of trusted applications in the window that opens (see fig. 8).

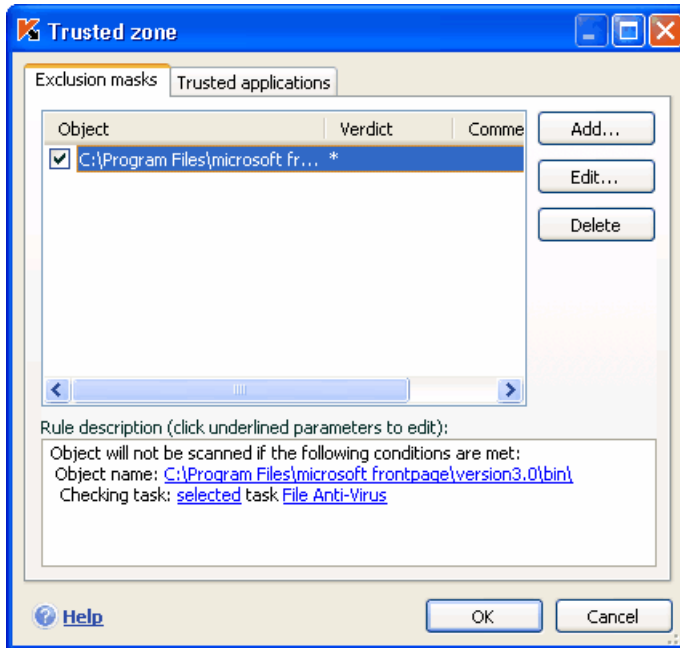


Figure 8. Creating a trusted zone

6.3.1. Exclusion rules

Exclusion rules are sets of conditions that Kaspersky Anti-Virus uses to determine not to scan an object.

You can exclude files of certain formats from the scan, use a file mask, or exclude a certain area, such as a folder or a program, program processes, or objects according to their Virus Encyclopedia classification.

The *classification* is the status that Kaspersky Anti-Virus assigns to an object during the scan. A status is assigned based on classification of malicious and potentially dangerous programs founded in the Kaspersky Lab Virus Encyclopedia.

Potentially dangerous software does not have a malicious function but can be used as an auxiliary component for a malicious code, since it contains holes and errors. This category includes, for example, remote administration programs, IRC

clients, FTP servers, all-purpose utilities for stopping or hiding processes, keyloggers, password macros, autodialers, etc. These programs are not classified as viruses. They can be divided into several types, e.g. Adware, Jokes, Riskware, etc. (for more information on potentially dangerous programs detected by Kaspersky Anti-Virus, see the Virus Encyclopedia at www.viruslist.com). After the scan, these programs may be blocked. Since several of them are very common, you have the option of excluding them from the scan. To do so, you must add the name or mask of the object to the trusted zone using the Virus Encyclopedia classification.

For example, imagine you use a Remote Administrator program frequently in your work. This is a remote access system with which you can work from a remote computer. Kaspersky Anti-Virus views this sort of application activity as potentially dangerous and may block it. To keep the application from being blocked, you must create an exclusion rule that specifies not-a-virus:RemoteAdmin.Win32.RAdmin.22 as the classification.

When you add an exclusion, a rule is created that several program components (File Anti-Virus, Mail Anti-Virus, Proactive Defense) and virus scan tasks can later use. You can create exclusion rules in a special window that you can open from the program settings window, from the notice about detecting the object, and from the report window.

*To add exclusions on the **Exclusion Mask** tab:*

1. Click on the **Add** button in the **Exclusion Mask** tab.
2. In the window that opens (see fig. 9), click the exclusion type in the **Properties** section:
 - Object** – exclusion of a certain object, directory, or files that match a certain mask from scans.
 - Verdict** – excluding an object from the scan based on its status from the Virus Encyclopedia classification.

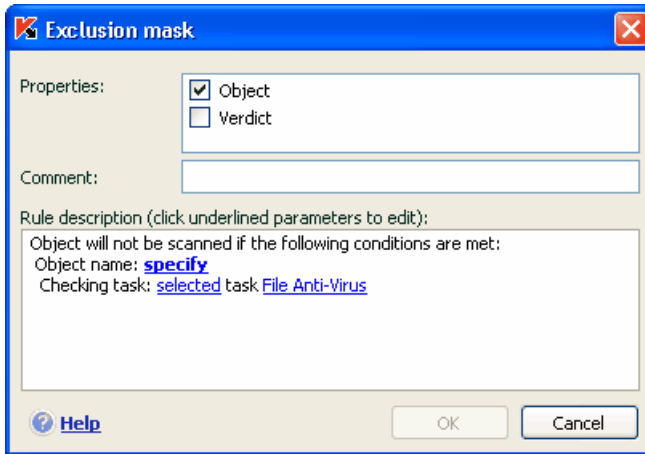


Figure 9. Creating an exclusion rule

If you check both boxes at once, a rule will be created that object with a certain Virus Encyclopedia classification. In such a case, the following rules apply:

- If you specify a certain file as the **Object** and a certain status in the **Verdict** section, the file specified will only be an exclusion if during the scan it is classified as the threat selected.
 - If you select an area or folder as the **Object** and the status (or mask) as the **Verdict**, then objects with that status will only be excluded from the scan in that area or folder.
3. Assign values to the selected exclusion types. To do so, left-click in the **Rule description** section on the specify link located next to the exclusion type:
- For the **Object** type, enter its name in the window that opens (this can be a file, a particular directory, or a file mask (see A.2 on pg. 209). Check **Include subfolders** for the object (file, file mask, folder) to be recursively excluded from the scan. For example, if you assign **C:\Program Files\winword.exe** as an exclusion and checked the subfolder option, the file **winword.exe** will be excluded from the scan if found in any **C:\Program Files** subfolders.
 - Enter the full name of the threat that you want to exclude from scans as given in the Virus Encyclopedia or use a mask for the **Verdict** (see A.3 on pg. 208).

For some classifications, you can assign advanced conditions for applying rules in the **Advanced settings** field. In most cases, the program fills this field automatically when you add an exclusion rule from a Proactive Defense notice.

You can add advanced settings for the following verdicts, among others:

- *Invader* (injects into program processes). For this verdict, you can give a name, mask, or complete path to the object being injected into (for example, a .dll file) as an additional exclusion condition.
 - *Opening Internet Browser*. For this verdict, you can list browser open settings as additional exclusion settings. For example, you blocked browsers from opening with certain settings in the Proactive Defense application activity analysis. However, you want to allow the browser to open for the domain *www.kaspersky.com* with a link from Microsoft Office Outlook as an exclusion rule. To do so, select Outlook as the exclusion **Object** and *Opening Internet Browser* as the **Verdict**, and enter an allowed domain mask in the **Advanced settings** field.
4. Define which Kaspersky Anti-Virus components will use this rule. If any is selected, this rule will apply to all components. If you want to restrict the rule to one or several components, click on any, which will change to selected. In the window that opens, check the boxes for the components that you want this exclusion rule to apply to.

To create an exclusion rule from a program notice stating that it has detected a dangerous object:

1. Use the Add to Trusted Zone link in the notification window (see fig. 10).

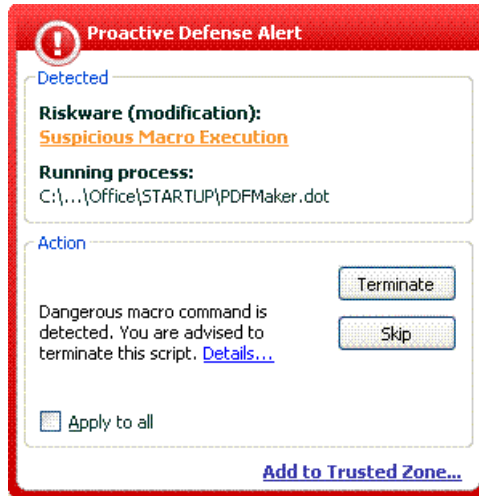


Figure 10. Dangerous object detection notification

2. In the window that opens, be sure that all the exclusion rule settings match your needs. The program will fill in the object name and threat type automatically, based on information from the notification. To create the rule, click **OK**.

To create an exclusion rule from the report window:

1. Select the object in the report that you want to add to the exclusions.
2. Open the context menu and select **Add to Trusted zone** (see fig. 11).
3. The exclusion settings window will then open. Be sure that all the exclusion rule settings match your needs. The program will fill in the object name and threat type automatically based on the information from the report. To create the rule, click **OK**.

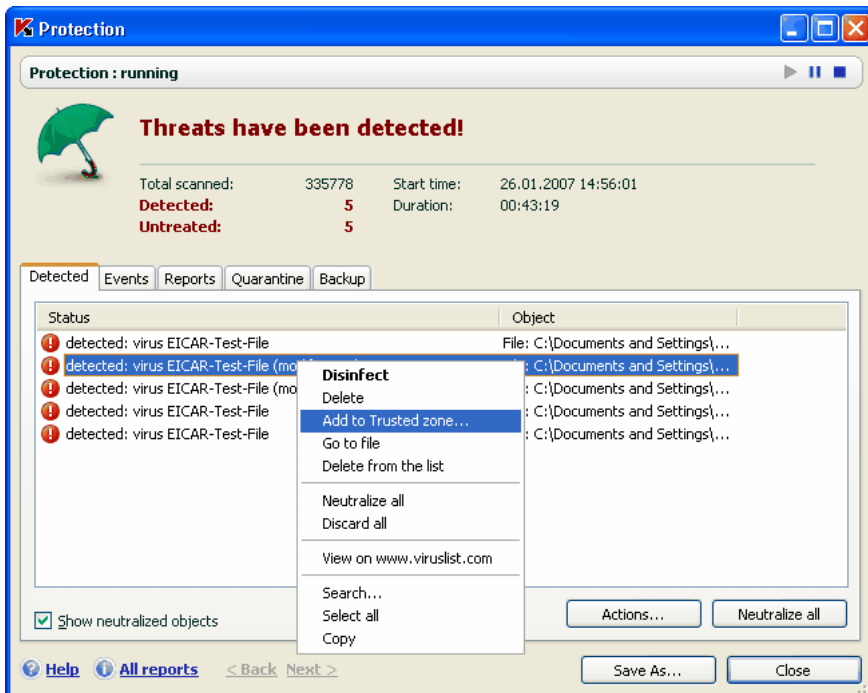


Figure 11. Creating an exclusion rule from a report

6.3.2. Trusted applications

You can only exclude trusted applications from the scan in Kaspersky Anti-Virus if installed on a computer running Microsoft Windows NT 4.0/2000/XP/Vista.

Kaspersky Anti-Virus can create a list of trusted applications, that need not have their file and network activity monitored, suspicious or otherwise.

For example, you feel that objects and processes used by Windows Notepad are safe and do not need to be scanned. To exclude objects used by this process from scanning, add Notebook to the trusted applications list. However, the executable file and the trusted application process will be scanned for viruses as before. To fully exclude the application from scanning, you must use exclusion rules (see 6.3.1 on pg. 60).

In addition, some actions classified as dangerous are perfectly normal features for a number of programs. For example, keyboard layout toggling programs regularly intercept text entered on your keyboard. To accommodate such

programs and stop monitoring their activity, you are advised to add them to the trusted application list.

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

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

You can create a list of trusted applications on the special **Trusted applications** tab (see Figure 12) This list contains by default a list of applications that will not be monitored based on Kaspersky Lab recommendations when you install Kaspersky Anti-Virus. If you do not trust an application on the list, deselect the corresponding checkbox. You can edit the list using the **Add**, **Edit**, and **Delete** buttons on the right.

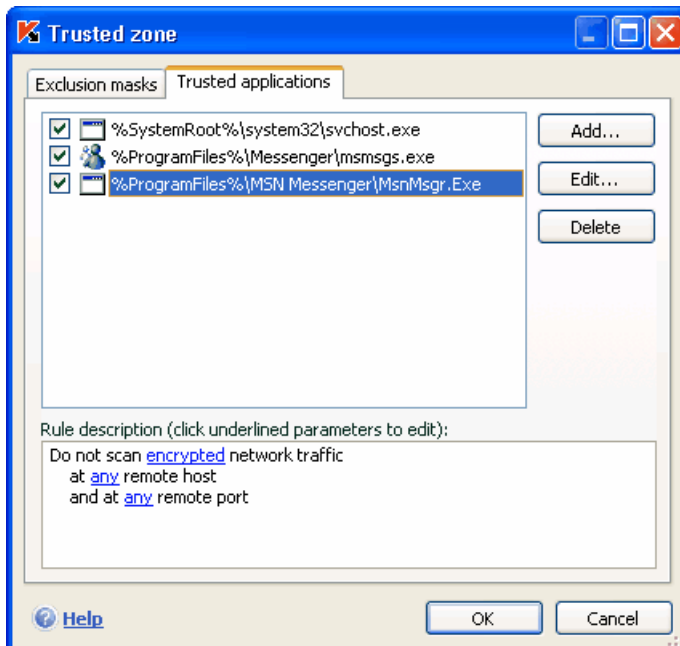


Figure 12. Trusted application list

To add a program to the trusted application list:

1. Click the **Add** button on the right-hand part of the window.
2. In the **Trusted application** window (see fig. 13) that opens, select the application using the **Browse** button. A context menu will open, and by clicking **Browse** you can go to the file selection window and select the path to the executable file, or by clicking **Applications** you can go to a list of applications currently running and select them as necessary.

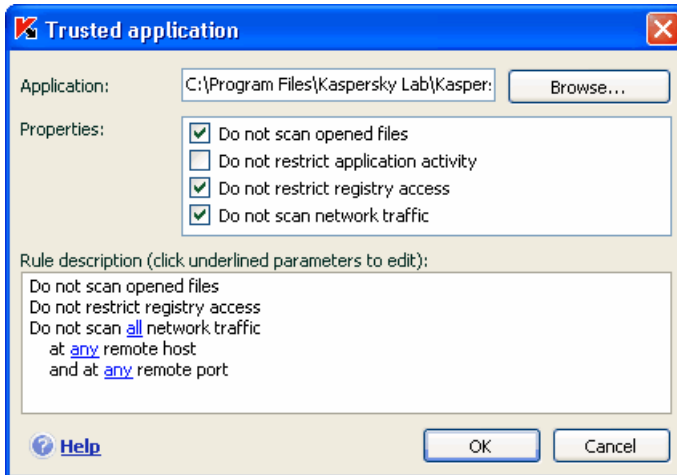


Figure 13. Adding an application to the trusted list

When you select a program, Kaspersky Anti-Virus records the internal attributes of the executable file and uses them to identify the trusted program during scans.

The file path is inserted automatically when you select its name.

3. Specify which actions performed by this process will not be monitored:
 - Do not scan opened files** – excludes from the scan all files that the trusted application process.
 - Do not restrict application activity** – excludes from Proactive Defense monitoring any activity, suspicious or otherwise, that the trusted application performs.
 - Do not restrict registry access** – excludes from scanning any accesses of the system registry initiated by the trusted application.

- Do not scan network traffic** – excludes from scans for viruses and spam any network traffic initiated by the trusted application . You can exclude all the application's network traffic or encrypted traffic (SSL) from the scan. To do so, click the [all](#) link. It will change to [encrypted](#). In addition you can restrict the exclusion by assigning a remote host/port. To create a restriction, click [any](#), which will change to [selected](#), and enter a value for the remote port/host.

6.4. Starting virus scan and update tasks under another user account

Note that this feature is unavailable in Microsoft Windows 98/ME.

Kaspersky Anti-Virus 6.0 has a feature that can start scan tasks under another user account. This feature is by default disabled, and tasks are run under the account under which you are logged into the system.

The feature is useful if for example, you need access rights to a certain object during a scan. By using this feature, you can configure tasks to run under a user that has the necessary privileges.

Program updates may be made from a source to which you do not have access (for example, the network update folder) or authorized user rights for a proxy server. You can use this feature to run the Updater with another account that has those rights.

To configure a scan task that starts under a different user account:

1. Select the task name in the **Scan (Service)** section of the main window and use the [Settings](#) link to open the task settings window.
2. Click the **Customize..** button in the task settings window and go to the **Additional** tab in the window that opens (see fig. 14).

To enable this feature, check **Run this task as**. Enter the data for the login that you want to start the task as below: user name and password.

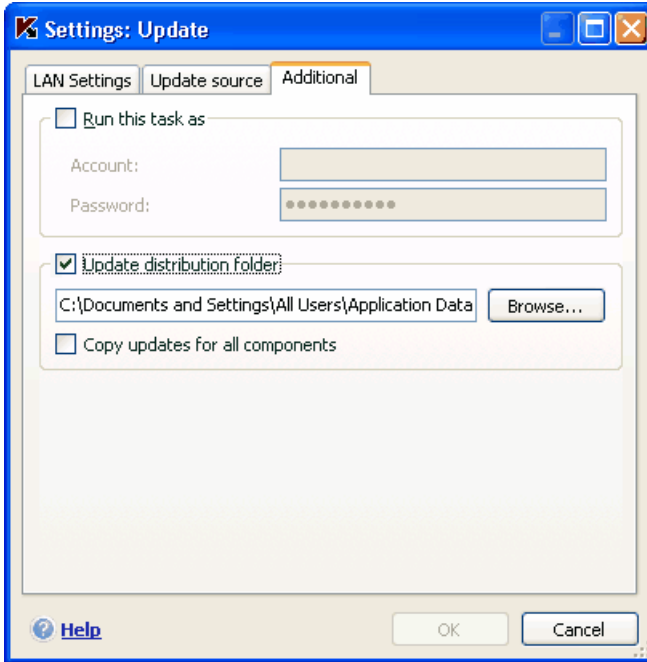


Figure 14. Configuring an update task from another profile

6.5. Configuring virus scan and update schedules

You can run virus scan and update tasks manually, or automatically using a schedule.

Virus scans preinstalled with the application are started automatically according to a selected schedule. Similarly scheduling is switched off for the update tasks created during installation. The Updater runs automatically as updates are released on the Kaspersky Lab servers.

To alter schedule settings, select the task name in the main program window in the **Scan** section (for virus scans) or the **Service** section (for update tasks) and open the settings window by clicking Settings.

To have tasks start according to a schedule, check the automatic task start box in the **Run Mode** section. You can edit the times for starting the scan task in the **Schedule** window (see Figure 15), that opens when you click **C**hange.

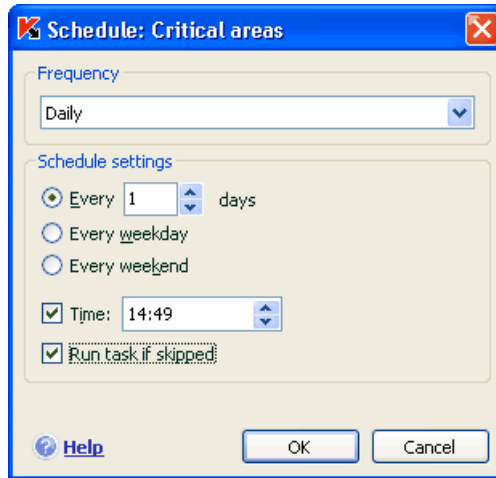




Figure 15. Configuring a task schedule

The most important step is to determine the frequency at which the task starts. You can select one of these options:

- At a specified time.** The task will run once on the day and at the time that you specify.
- On program startup.** The task starts up every time Kaspersky Anti-Virus is run.
- After each update.** The task starts after each threat signature update (this only applies to virus scan tasks).
- Minutely.** The time interval between scans will be a number of minutes, not greater than 59. Specify the number of minutes between scans in the schedule settings.
- Hourly.** The interval between scans is calculated in hours. Enter the number of hours in the schedule settings: **Every n -th hour** and enter the value for n . For example, enter **Every 1 hour** if you want the task to run hourly.
- Daily** – the period between scans is calculated in days. Specify how often the scan should run in the schedule settings:
 - Select the **Every n -th day** option and enter a value for n . Enter *Every 2 days* if you want to run the scan every other day.
 - Select **Every weekday** if you want the scan to run daily, Monday through Friday.
 - Select **Every weekend** for the task to run on Saturdays and Sundays only.

In addition to the frequency, specify what time of day or night the scan task will run in the **Time** field.

-  **Weekly** – the scan task will run on certain days of the week. If you select this option, put checkmarks next to the days of the week that on which you want the scan to run in the schedule settings. Also enter the time at which the scan task will run in the *Time* field.
-  **Monthly** – the scan task will run once per month, at the specified day and time.

If a scan task is skipped for any reason (for example, the computer was not on at that time), you can configure the task that was missed to start automatically as soon as it can. To do so, check **Run task if skipped** in the schedule window.

6.6. Power options

To conserve the battery of your laptop computer, and to reduce the load on the central processor and disk subsystems, you can postpone virus scans:

- Since virus scans and program updates sometimes require a fair amount of resources and can take up time, you are advised to disable schedules for these tasks, which will help you to save battery life. If necessary, you can manually update the program yourself (see 5.5 on pg. 52) or start a virus scan. To use the battery-saving feature, check **Disable scheduled scans while running on battery power**.
- Virus scans increase the load on the central processor and disk subsystems, thereby slowing down other programs. By default, if such a situation arises, the program pauses virus scans and frees up system resources for user applications.

However, there are a number of programs that can be launched as soon as the processor's resources are freed and run in background mode. For virus scans not to depend on the operation of such programs, uncheck **Concede resources to other applications**.

Note that this setting can be configured individually for every virus scan task. If you choose to do this, the configuration for a specific task has a higher priority.

To configure power settings for virus scan tasks:

Select the **Protection** section of the main program window and click the Settings link. Configure power settings in the **Additional** box (see fig. 16).

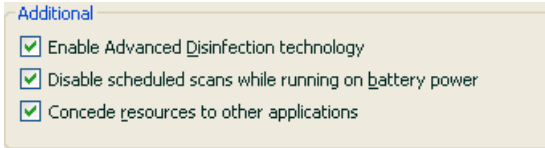


Figure 16. Power options

6.7. Advanced Disinfection Technology

Today's malicious programs can invade the lowest levels of an operating system, which makes them practically impossible to delete. Kaspersky Anti-Virus 6.0 asks you if you want to run Advanced Disinfection Technology when it detects a threat currently active in the system. This will neutralize the threat and delete it from the computer.


After this procedure, you will need to restart your computer. After restarting your computer, we recommend running a full virus scan (see 5.2 on pg. 50). To use Advanced Disinfection Technology, check **Enable Advanced Disinfection technology**.

To enable/disable advanced disinfection technology:

Select the **Protection** section of the main program window and click the Settings link. Configure power settings in the **Additional** box (see fig.16).

CHAPTER 7. FILE ANTI-VIRUS

The Kaspersky Anti-Virus component that protect your computer files against infection is called *File Anti-Virus*. It loads when you start your operating system, runs in your computer's RAM, and scans all files opened, saved, or executed.

The component's activity is indicated by the Kaspersky Anti-Virus system tray icon, which looks like this  whenever a file is being scanned.

File Anti-Virus by default scans only *new or modified files*, that is, only files that have been added or changed since the previous scan. Files are scanned with the following algorithm:

1. Each file that the user or a program deals with is intercepted by the component.
2. File Anti-Virus scans the iChecker™ and iSwift™ databases for information on the file intercepted. A decision is made whether to scan the file based on the information retrieved.

The scanning process includes the following steps:

1. The file is analyzed for viruses. Malicious objects are detected by comparison with the program's *threat signatures*, which contain descriptions of all malicious programs, threats, and network attacks known to date, with methods for neutralizing them.
2. After the analysis, there are three available courses of action:
 - a. If malicious code is detected in the file, File Anti-Virus blocks the file, places a copy of it in *Backup*, and attempts to disinfect the file. If the file is successfully disinfected, it becomes available again. If not, the file is deleted.
 - b. If code is detected in a file that appears to be malicious but there is no guarantee, the file is subject to disinfection and is sent to *Quarantine*.
 - c. If no malicious code is discovered in the file, it is immediately restored.

7.1. Selecting a file security level

File Anti-Virus protects files that you are using at one of the following levels (see fig. 17):

High – the level with the most comprehensive monitoring of files opened, saved, or run.

Recommended – Kaspersky Lab recommends this settings level. It will scan the following object categories:

- Programs and files by contents
- New objects and objects modified since the last scan
- Embedded OLE objects

Low – level with settings that let you comfortably use applications that require significant system resources, since the scope of files scanned is reduced.

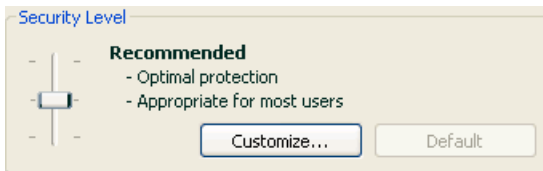


Figure 17. File Anti-Virus security level

The default setting for File Anti-Virus is **Recommended**.

You can raise or lower the protection level for files you use by either selecting the level you want, or changing the settings for the current level.

To change the security level:

Adjust the sliders. By adjusting the security level, you define the ratio of scan speed to the total number of files scanned: the fewer files are scanned for viruses, the higher the scan speed.

If none of the set file security levels meet your needs, you can customize the protection settings. To do so, select the level that is closest to what you need as a starting point and edit its settings. In such a case, the level will be set at **Custom settings**. Let's look at an example of when user defined file security levels could be useful.

Example:

The work you do on your computer uses a large number of file types, and some the files may be fairly large. You would not want to run the risk of skipping any files in the scan because of the size or extension, even if this would somewhat affect the productivity of your computer.

Tip for selecting a level:

Based on the source data, one can conclude that you have a fairly high risk of being infected by a malicious program. The size and type of the files being handled is quite varied and skipping them in the scan would

put your data at risk. You want to scan the files you use by contents, not by extension.

You are advised to start with the **Recommended** security level and make the following changes: remove the restriction on scanned file sizes and optimize File Anti-Virus operation by only scanning new and modified files. Then the scan will not take up as many system resources so you can comfortably use other applications.

To modify the settings for a security level:

Click the **Customize** button in the File Anti-Virus settings window. Edit the File Anti-Virus settings in the window that opens and click **OK**.

As a result, a fourth security level will be created, **Custom**, which contains the protection settings that you configured.

7.2. Configuring File Anti-Virus

Your settings determine how File Anti-Virus will defend your computer. The settings can be broken down into the following groups:

- Settings that define what file types (see 7.2.1 on pg. 75) are to be scanned for viruses
- Settings that define the scope of protection (see 7.2.2 on pg. 78)
- Settings that define how the program responds to dangerous objects (see 7.2.5 on pg. 82)
- additional File Anti-Virus settings (see 7.2.3 on pg. 79)

The following sections will examine these groups in detail.

7.2.1. Defining the file types to be scanned

When you select file types to be scanned, you establish what file formats, sizes, and what drives will be scanned for viruses when opened, executed, or saved.

To make configuration easier, all files are divided into two groups: *simple* and *compound*. Simple files, for example, .txt files, do not contain any objects. Compound objects can include several objects, each of which may in turn contain other objects. There are many examples: archives, files containing macros, spreadsheets, emails with attachments, etc.

The file types scanned are defined in the **File types** section (see Figure 18). Select one of the three options:

- ④ **Scan all files.** With this option selected, all file system objects that are opened, run, or saved will be scanned without exceptions.
- ④ **Scan programs and documents (by content).** If you select this group of files, File Anti-Virus will only scan potentially infected files – files that a virus could imbed itself in.

Note:

There are a number of file formats that have a fairly low risk of having malicious code injected into them and subsequently being activated. An example would be .txt files.

And vice versa, there are file formats that contain or can contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of injection and activation of malicious code in such files is fairly high.

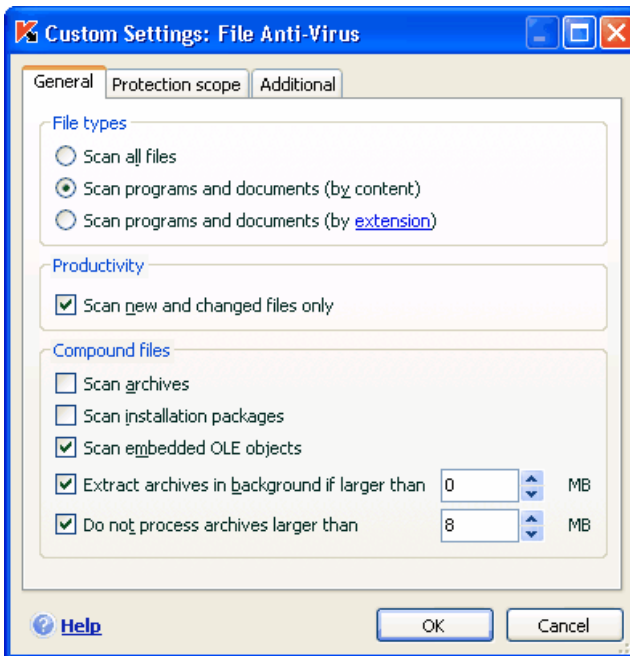



Figure 18. Selecting the file types scanned for viruses

Before searching for viruses in a file, its internal header is analyzed for the file format (txt, doc, exe, etc.). If the analysis shows that the file format cannot be infected, it is not scanned for viruses and is immediately returned to the user. If the file format can be infected, the file is scanned for viruses.

-  **Scan programs and documents (by extension).** If you select this option, File Anti-Virus will only scan potentially infected files, but the file format will be determined by the filename's extension. Using the extension link, you can review a list of file extensions (see A.1 on pg. 206) that are scanned with this option.

Tip:

Do not forget that someone could send a virus to your computer with an extension (e.g. .txt) that is actually an executable file renamed as a .txt file. If you select **Scan programs and documents (by extension)**, the scan would skip such a file. If **Scan programs and documents (by content)** is selected, the extension is ignored, and analysis of the file headers will uncover that the file is an .exe file. File Anti-Virus would thoroughly scan the file for viruses.

In the **Productivity** section, you can specify that only new and modified files should be scanned for viruses. This mode noticeably reduces scan time and increases the program's performance speed. To select this mode, check **Scan new and changed files only.** This mode applies to both simple and compound files.

In the **Compound files** section, specify which compound files to scan for viruses:

- Scan archives** – scans .zip, .cab, .rar, and .arj archives.
- Scan installation packages** – scans self-extracting archives for viruses.
- Scan embedded OLE objects** – scans objects embedded in files (for example, Excel spreadsheets or macros imbedded in a Microsoft Word file, email attachments, etc.).

You can select and scan all files, or only new files, for each type of compound file. To do so, left-click the link next to the name of the object to toggle its value. If the **Productivity** section has been set up only to scan new and modified files, you will not be able to select the type of compound files to be scanned.

To specify compound files that should not be scanned for viruses, use the following settings:

- Extract archives in background if larger than... MB.** If the size of a compound object exceeds this restriction, the program will scan it as a single object (by analyzing the header) and will return it to the user. The objects that it contains will be scanned later. If this option is not checked, access to files larger than the size indicated will be blocked until they have been scanned.
- Do not process archives larger than... MB.** With this option checked, files larger than the size specified will be skipped by the scan.

7.2.2. Defining protection scope

By default, File Anti-Virus scans all files when they are used, regardless of where they are stored, whether it be a hard drive, CD/DVD-ROM, or flash drive.

You can limit the scope of protection. To do so:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking **Settings**.
2. Click the **Customize** button and select the **Protection scope** tab (see fig. 19) in the window that opens.

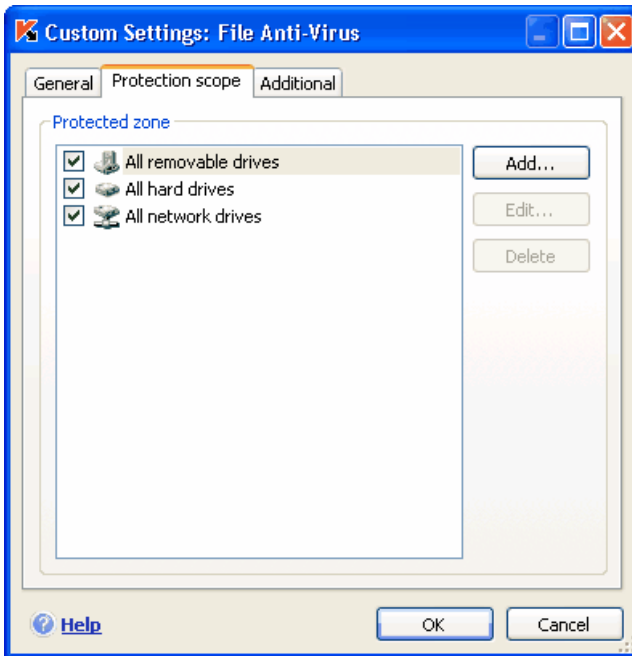


Figure 19. Creating a protected zone

The tab displays a list of objects that File Anti-Virus will scan. Protection is enabled by default for all objects on hard drives, removable media, and network drives connected to your computer. You can add to and edit the list using the **Add**, **Edit**, and **Delete** buttons.

If you want to protect fewer objects, you can do so using the following methods:

- Specify only folders, drives, and files that need to be protected.

- Create a list of objects that do not need to be protected.
- Combine methods one and two – create a protection scope that excludes a number of objects.

You can use masks when you add objects for scanning. Note that you can only enter masks with absolute paths to objects:

- **C:\dir\.*** or **C:\dir*** or **C:\dir** - all files in folder *C:\dir*
- **C:\dir*.exe** - all files with the extension *.exe* in the folder *C:\dir*
- **C:\dir*.ex?** – all files with the extension *.ex?* in the folder *C:\dir*, where *?* can represent any one character
- **C:\dir\test** – only the file *C:\dir\test*

In order for the scan to be carried out recursively, check **Include subfolders**.

Warning!

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

7.2.3. Configuring advanced settings

As additional File Anti-Virus settings, you can specify the file system scanning mode and configure the conditions for temporarily pausing the component.

To configure additional File Anti-Virus settings:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking the Settings link.
2. Click the **Customize** button and select the **Additional** tab in the window that opens (see Figure 20).

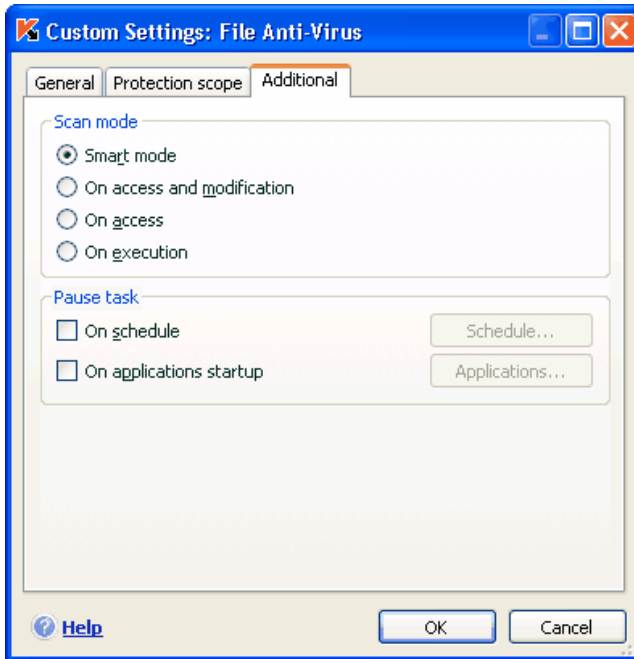


Figure 20. Configuring additional File Anti-Virus settings

The file scanning mode determines the File Anti-Virus processing conditions. You have following options:

- **Smart mode.** This mode is aimed at speeding up file processing and return them to the user. When it is selected, a decision to scan is made based on analyzing the operations performed with the file.

For example, when using a Microsoft Office file, Kaspersky Anti-Virus scans the file when it is first opened and last closed. All operations in between that overwrite the file are not scanned.

Smart mode is the default.

- **On access and modification** – File Anti-Virus scans files as they are opened or edited.
- **On access** – only scans files when an attempt is made to open them.
- **On execution** – only scans files when an attempt is made to run them.

You might need to pause File Anti-Virus when performing tasks that require significant operating system resources. To lower the load and ensure that the

user regains access to files quickly, we recommend configuring the component to disable at a certain time or while certain programs are used.

To pause the component for a certain length of time, check **On schedule** and in the window that opens (see Figure 8) click **Schedule** to assign a time frame for disabling and resuming the component. To do so, enter a value in the format HH:MM in the corresponding fields.

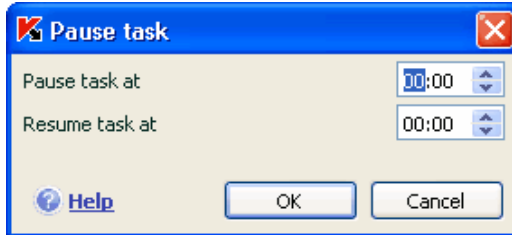


Figure 21. Pausing the component

To disable the component when working with programs that require significant resources, check **On applications startup** and edit the list of programs in the window that opens (see Figure 22) by clicking **Applications**.

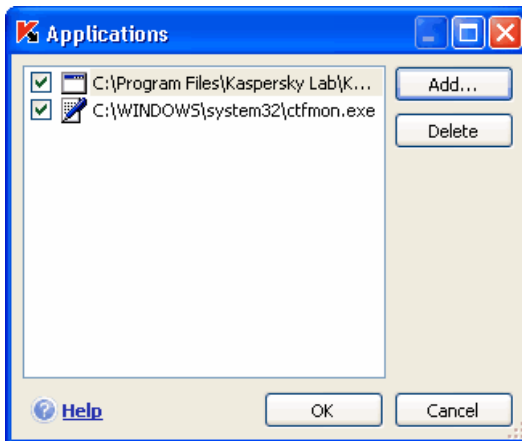


Figure 22. Creating an application list

To add an application to the list, use the **Add** button. A context menu will open, and by clicking **Browse** you can go to the standard file selection window and specify the executable file the application to add. Or, go to the list of applications currently running from the **Applications** item and select the one you want.

To delete an application, select it from a list and click **Delete**.

You can temporarily disable the pause on File Anti-Virus when using a specific application. To do so, uncheck the name of the application. You do not have to delete it from the list.

7.2.4. Restoring default File Anti-Virus settings

When configuring File Anti-Virus, you can always return to the default performance settings. Kaspersky Lab considers them to be optimal and has combined them in the **Recommended** security level.

To restore the default File Anti-Virus settings:

1. Select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Default** button in the **Security Level** section.

If you modified the list of objects included in the protected zone when configuring File Anti-Virus settings, the program will ask you if you want to save that list for future use when you restore the initial settings. To save the list of objects, check **Protected Zone** in the **Restore Settings** window that opens.

7.2.5. Selecting actions for objects

If File Anti-Virus discovers or suspects an infection in a file while scanning it for viruses, the program's next steps depend on the object's status and the action selected.

File Anti-Virus can label an object with one of the following statuses:

- Malicious program status (for example, *virus*, *Trojan*).
- *Potentially infected*, when the scan cannot determine whether the object is infected. This means that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, all infected files are subject to disinfection, and if they are potentially infected, they are sent to Quarantine.

To edit an action for an object:

select **File Anti-Virus** in the main window and go to the component settings window by clicking Settings. All potential actions are displayed in the appropriate sections (see fig. 23).

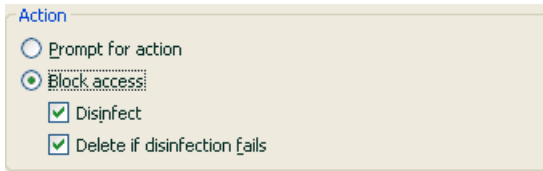


Figure 23. Possible File Anti-Virus actions with dangerous objects

| If the action selected was | When it detects a dangerous object |
|--|--|
| <input type="radio"/> Prompt for action | File Anti-Virus issues a warning message containing information about what malicious program has infected or potentially infected the file, and gives you a choice of actions. The choice can vary depending on the status of the object. |
| <input type="radio"/> Block access | File Anti-Virus blocks access to the object. Information about this is recorded in the report (see 14.3 on pg. 158). Later you can attempt to disinfect this object. |
| <input type="radio"/> Block access <input checked="" type="checkbox"/> Disinfect | File Anti-Virus will block access to the object and will attempt to disinfect it. If disinfection fails, the file will be assigned the status of <i>potentially infected</i> , and it will be moved to Quarantine (see 14.1 on pg. 153). Information about this is recorded in the report. Later you can attempt to disinfect this object. |
| <input type="radio"/> Block access <input checked="" type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete if disinfection fails | File Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be disinfected, it is deleted. A copy of the object will be stored in Backup (see 14.2 on pg. 156). |
| <input type="radio"/> Block access | File Anti-Virus will block access to the |

| If the action selected was | When it detects a dangerous object |
|---|------------------------------------|
| <input checked="" type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete | object and will delete it. |

When disinfecting or deleting an object, Kaspersky Anti-Virus creates a backup copy and sends it to Backup in case the object needs to be restored or an opportunity arises to treat it.

7.3. Postponed disinfection

If you select **Block access** as the action for malicious programs, the objects will not be treated and access to them will be blocked.

If the actions selected were

- Block access**
- Disinfect**

all untreated objects will also be blocked.


In order to regain access to blocked objects, they must be disinfecting. To do so:

1. Select **File Anti-Virus** in the main window of the program and left-click anywhere in the **Statistics** box.
2. Select the objects that interest you on the **Detected** tab and click the **Actions** → **Neutralize all** button.

Successfully disinfecting files will be returned to the user. Any that cannot be treated, you can *delete* or *skip* it. In the latter case, access to the file will be restored. However, this significantly increases the risk of infection on your computer. It is strongly recommended not to skip malicious objects.

CHAPTER 8. MAIL ANTI-VIRUS

Mail Anti-Virus is Kaspersky Anti-Virus's component to prevent incoming and outgoing email from transferring dangerous objects. It starts running when the operating system boots up, stays active in your system memory, and scans all email on protocols POP3, SMTP, IMAP, MAPI¹ and NNTP, as well as encryption for POP3 and IMAP (SSL).

The component's activity is indicated by the Kaspersky Anti-Virus system tray icon, which looks like this  whenever an email is being scanned.

The default setup for Mail Anti-Virus is as follows:

1. Mail Anti-Virus intercepts each email received or sent by the user.
2. The email is broken down into its parts: email headers, its body, and attachments.
3. The body and attachments of the email (including OLE attachments) are scanned for dangerous objects. Malicious objects are detected using the *threat signatures* included in the program, and with the heuristic algorithm. The signatures contain descriptions of all the malicious programs known to date and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the threat signatures.
4. After the virus scan, you have the following available courses of action:
 - if the body or attachments of the email contain malicious code, Mail Anti-Virus will block the email, place a copy of the infected object in *Backup*, and try to disinfect the object. If the email is successfully disinfected, it becomes available to the user again. If not, the infected object in the email is deleted. After the virus scan, special text is inserted in the subject line of the email stating that the email has been processed by Kaspersky Anti-Virus.
 - If code is detected in the body or an attachment that appears to be, but is not definitely, malicious, the suspicious part of the email is sent to *Quarantine*.

¹ Emails sent with MAPI are scanned using a special plug-in for Microsoft Office Outlook and The Bat!

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

A special plug-in (see 8.2.2 on pg. 89) is provided for Microsoft Outlook that can configure email scans more exactly.

If you use The Bat!, Kaspersky Anti-Virus can be used in conjunction with other anti-virus applications. The rules for processing email traffic (see 8.2.3 on pg. 91) are configured directly in The Bat! and supersede the Kaspersky Anti-Virus email protection settings.

When working with other email programs, including Outlook Express, Mozilla Thunderbird, Eudora, Incredimail, Mail Anti-Virus scans email on SMTP, POP3, IMAP, MAPI, and NNTP protocols.

8.1. Selecting an email protection level

Kaspersky Anti-Virus protects your email at one of these levels (see fig. 24):

High – the level with the most comprehensive monitoring of incoming and outgoing emails. The program scans email attachments, including archives, in detail, regardless of how long the scan takes.

Recommended – Kaspersky Lab experts recommend this level. It scans the same objects as **High**, with the exception of attachments or emails that will take more than three minutes to scan.

Low – the security level with settings that let you comfortably use resource-intensive applications, since the scope of email scanning is limited. Thus, only your incoming email is scanned on this level, and in doing so archives and objects (emails) attached are not scanned if they take more than three minutes to scan. This level is recommended if you have additional email protection software installed on your computer.

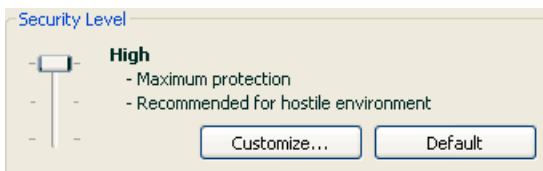


Figure 24. Selecting an email security level

By default, the email security level is set to **Recommended**.

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

To change the security level:

Adjust the sliders. By altering the security level, you define the ratio of scan speed to the total number of objects scanned: the fewer email objects are scanned for dangerous objects, the higher the scan speed.

If none of the preinstalled levels meets your needs, you can edit its settings. If you do, the level will be set to **Custom settings**. Let's look at an example of when user defined email security levels could be useful.

Example:

Your computer is outside the local area network and uses a dial-up Internet connection. You use Outlook Express as an email client for receiving and sending email, and you use a free email service. For a number of reasons, your email contains archived attachments. How do you maximally protect your computer from infection through email?

Tip for selecting a level:

By analyzing your situation, one can conclude that you are at a high risk of infection through email in the scenario outlined, because there is no centralized email protection and through using a dial-up connection.

You are advised to use **High** as your starting point, with the following changes: reduce the scan time for attachments to, for example, 1-2 minutes. The majority of archived attachments will be scanned for viruses and the processing speed will not be seriously slowed.

To modify a preinstalled security level:

Click the **Customize** button in the Mail Anti-Virus settings window. Edit the email protection settings in the window that opens, and click **OK**.

8.2. Configuring Mail Anti-Virus

A series of settings govern how your email is scanned. The settings can be broken down into the following groups:

- Settings that define the protected group (see 8.2.1 on pg. 88) of emails
- Email scan settings for Microsoft Outlook (see 8.2.2 on pg. 89) and The Bat! (see 8.2.3 on pg. 91)

Warning!

This version of Kaspersky Anti-Virus does not provide Mail Anti-Virus plug-ins for 64-bit mail clients.

- settings that define actions for dangerous email objects (see 8.2.4 on pg. 92)

The following sections examine these settings in detail.

8.2.1. Selecting a protected email group

Mail Anti-Virus allows you to select exactly what group of emails to scan for dangerous objects.

By default, the component protects email at the **Recommended** security level, which means scanning both incoming and outgoing email. When you first begin working with the program, you are advised to scan outgoing email, since it is possible that there are worms on your computer that use email as a channel for distributing themselves. This will help avoid the possibility of unmonitored mass mailings of infected emails from your computer.

If you are certain that the emails that you are sending do not contain dangerous objects, you can disable the outgoing email scan. To do so:

1. Select **Mail Anti-Virus** in the main window and go to the component settings window by clicking Settings. Click on the **Customize** button in the Mail Anti-Virus configuration window.
2. In the Mail Anti-Virus Custom settings window that opens (see fig.), select **Only incoming mail** in the **Scope** section.

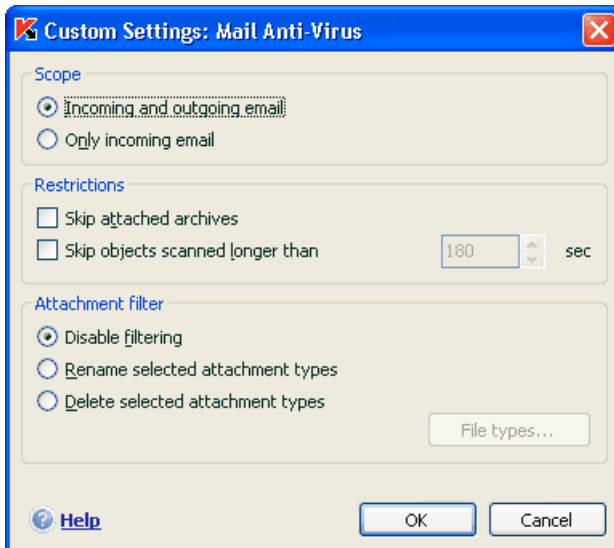


Figure 25. Mail Anti-Virus settings

In addition to selecting an email group, you can specify whether archived attachments should be scanned, and also set the maximum amount of time for scanning a single email object. These settings are configured in the **Restrictions** section.

If your computer is not protected by any local network software, and accesses the Internet without using a proxy server or firewall, you are advised **not to disable** the archived attachment scan and not to set a time limit on scanning.

If you are working in a protected environment, you can change the time restrictions on scanning to increase the email scan speed.

You can configure the filtration conditions for objects connected to an email in the **Attachment filter** section:

- ① **Disable filtering** – do not use additional filtration for attachments.
- ② **Rename selected attachment types** – filter out a certain attachment format and replace the last character of the file name with an underscore. You can select the file type by clicking the File types button.
- ③ **Delete selected attachment types** – filter out and delete a certain attachment format. You can select the file type by clicking the File types button.

You can find more information about filtered attachment types in section A.1 on pg. 206.

By using the filter, you increase your computer's security, since malicious programs spread through email most frequently as attachments. By renaming or deleting certain attachment types, you protect your computer against automatically opening attachments when a message is received.

8.2.2. Configuring email processing in Microsoft Office Outlook

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

A special plug-in is installed in Outlook when you install Kaspersky Anti-Virus. It can quickly access Mail Anti-Virus settings, and also set the maximum time that individual emails will be scanned for dangerous objects.

Warning!

This version of Kaspersky Anti-Virus does not provide Mail Anti-Virus plug-ins for 64-bit Microsoft Office Outlook.

The plug-in comes in the form of a special **Mail Anti-Virus** tab located under **Service → Options** (see fig. 26).

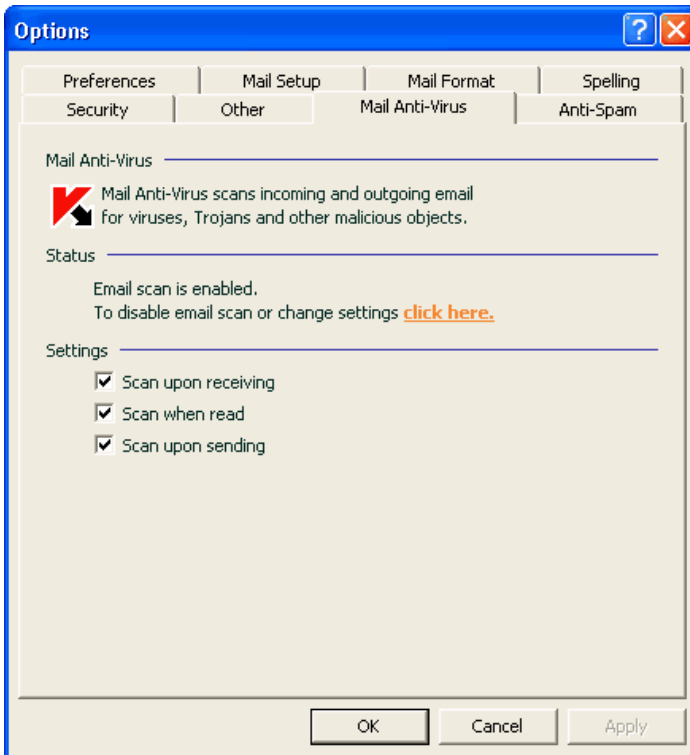


Figure 26. Configuring Mail Anti-Virus settings in Microsoft Outlook

Select an email scan mode:

- Scan upon receiving** – analyzes each email when it enters your Inbox.
- Scan when read** – scans each email when you open it to read it.
- Scan upon sending** – scans each email for viruses when you send it.

Warning!

If you use Outlook to connect to your email service on IMAP, you are advised not to use **Scan upon receiving** mode. Enabling this mode will lead to emails being copied to the local computer when delivered to the server, and consequently the main advantage of IMAP is lost – creating less traffic and dealing with unwanted email on the server without copying them to the user's computer.

The action that will be taken on dangerous email objects is set in the Mail Anti-Virus settings, which can be configured by following the [click here](#) link in the Status section.

8.2.3. Configuring email scans in The Bat!

Actions taken on infected email objects in The Bat! are defined with the program's own tools.

Warning!

The Mail Anti-Virus settings that determine whether incoming and outgoing email is scanned, as well as actions on dangerous email objects and exclusions, are ignored. The only settings that The Bat! takes into account relate to scanning archived attachments and time limits on scanning emails (see 8.2.1 on pg. 88).

The Mail Anti-Virus plug-in version for the 64-bit version of Microsoft Office Outlook is not available in this version of Kaspersky Anti-Virus.

To set up email protection rules in The Bat!:

1. Select **Preferences** from the email client's **Options** menu.
2. Select **Protection** from the settings tree.

The protection settings displayed (see Figure 27) extend to all anti-virus modules installed on the computer that support The Bat!

You must decide:

- What group of emails will be scanned for viruses (incoming, outgoing)
- At what point in time email objects will be scanned for viruses (when opening an email or before saving one to disk)
- The actions taken by the email client when dangerous objects are detected in emails. For example, you could select:

Try to cure infected parts – tries to treat the infected email object, and if the object cannot be disinfected, it stays in the email. Kaspersky Anti-Virus will always inform you if an email is infected. But even if you select **Delete** in the Mail Anti-Virus notice window, the object will remain in the email, since the action selected in The Bat! takes precedent over the actions of Mail Anti-Virus.

Remove infected parts – delete the dangerous object in the email, regardless of whether it is infected or suspected of being infected.

By default, The Bat! places all infected email objects in the Quarantine folder without treating them.

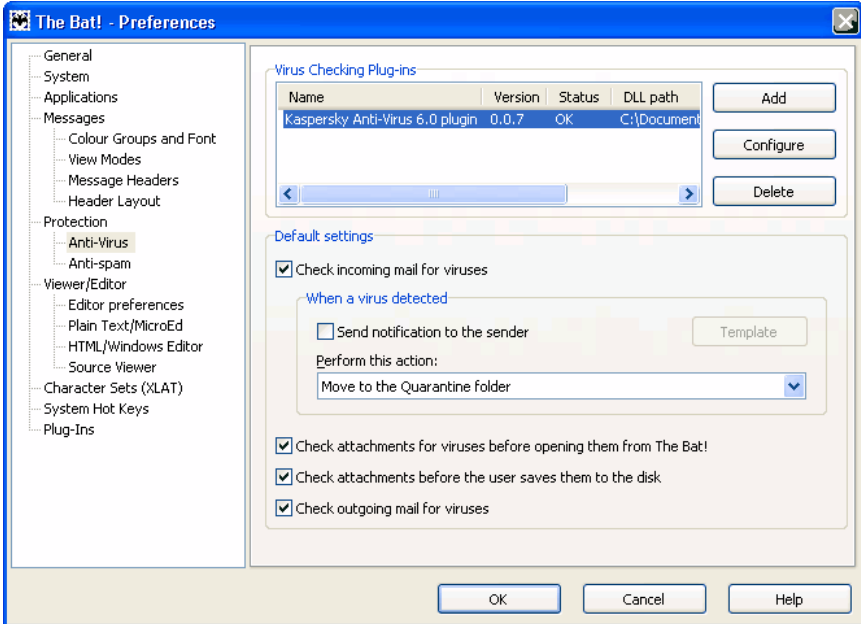


Figure 27. Configuring email scans in The Bat!

Warning!

The Bat! does not mark emails containing dangerous objects with special headers.

8.2.4. Restoring default Mail Anti-Virus settings

When configuring Mail Anti-Virus, you can always return to the default performance settings, which Kaspersky Lab considers to be optimal and has combined in the **Recommended** security level.

To restore the default Mail Anti-Virus settings:

1. Select **Mail Anti-Virus** in the main window and go to the component settings window by clicking Settings.
2. Click the **Default** button in the **Security Level** section.

8.2.5. Selecting actions for dangerous email objects

If a scan shows that an email or any of its parts (body, attachment) is infected or suspicious, the steps taken by Mail Anti-Virus depend on the object status and the action selected.

One of the following statuses can be assigned to the email object after the scan:

- Malicious program status (for example, *virus*, *Trojan* – for more details, see 1.1 on pg. 9).
- *Potentially infected*, when the scan cannot determine whether the object is infected. This means that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, when Mail Anti-Virus detects a dangerous or potentially infected object, it displays a warning on the screen and prompts the user to select an action for the object.

To edit an action for an object:

Open the Kaspersky Anti-Virus settings window and select **Mail Anti-Virus**. All possible actions for dangerous objects are listed in the **Action** box (see fig. 28).

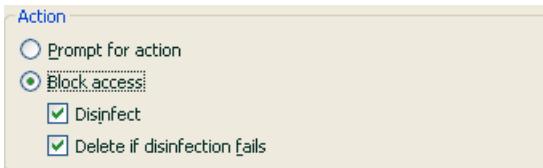


Figure 28. Selecting actions for dangerous email objects

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

| If the action selected was | When a dangerous object is detected |
|--|---|
| <input type="radio"/> Prompt for action | Mail Anti-Virus will issue a warning message containing information about what malicious program has infected (potentially infected) the file and will give you the choice of one of the following actions. |
| <input checked="" type="radio"/> Block access | E-Mail Anti-Virus blocks access to the |

| | |
|---|--|
| | object. Information about this is recorded in the report (see 14.3 on pg. 158). Later you can attempt to disinfect this object. |
| <input checked="" type="radio"/> Block access <input checked="" type="checkbox"/> Disinfect | E-Mail Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object could not be treated, it is moved to Quarantine. Information about this is recorded in the report. Later you can attempt to disinfect this object. |
| <input checked="" type="radio"/> Block access <input checked="" type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete if disinfection fails² | E-Mail Anti-Virus will block access to the object and will attempt to disinfect it. If it is successfully disinfected, it is restored for regular use. If the object cannot be disinfected, it is deleted. A copy of the object will be stored in Backup. Objects with the status of <i>potentially infected</i> will be moved to Quarantine. |
| <input checked="" type="radio"/> Block access <input type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete | When Mail Anti-Virus detects an infected or potentially infected object, it deletes it without informing the user. |

When disinfecting or deleting an object, Kaspersky Anti-Virus creates a backup copy and sends it to Backup (see 14.2 on pg. 156) before it attempts to treat the object or delete it, in case the object needs to be restored or an opportunity arises to treat it.

² If you are using The Bat! as your mail client, dangerous email objects will either be disinfected or deleted when Mail Anti-Virus takes this action (depending on the action selected in The Bat!).

CHAPTER 9. WEB ANTI-VIRUS


Whenever you use the Internet, information stored on your computer is open to the risk of infection by dangerous programs, which can penetrate your computer when you read an article on the Internet.

Web Anti-Virus is Kaspersky Anti-Virus's component for guarding your computer during Internet use. It protects information that enters your computer via the HTTP protocol, and also prevents dangerous scripts from being loaded on your computer.

Warning!

Web Anti-Virus only monitors HTTP traffic that passes through the ports listed on the monitored port list (see 14.7 on pg. 171). The ports most commonly used for transmitting email and HTTP traffic are listed in the program package. If you use ports that are not on this list, add them to it to protect traffic passing through them.


If you are working on an unprotected network, or using a modem for Internet access, you are advised to use *Web Anti-Virus* to protect yourself while using the Internet. Even if your computer is running on a network protected by a firewall or HTTP traffic filters, *Web Anti-Virus* provides additional protection while you browse the Web.

The component's activity is indicated by the Kaspersky Anti-Virus system tray icon, which looks like this  whenever scripts are being scanned.

Let's look at the component's operation in more detail.

Web Anti-Virus consists of two modules, that handle:

- *Traffic scan* – scans objects that enter the user's computer via HTTP.
- *Script scan* – scans all scripts processed by Microsoft Internet Explorer and any WSH scripts (JavaScript and Visual Basic Script), etc.) that are loaded while the user is on the computer and on the Internet.

A special plug-in for Microsoft Internet Explorer is installed as part of Kaspersky Anti-Virus installation. The  icon in the browser's Standard Buttons toolbar indicates that it is installed. Clicking on the icon opens an information panel with *Web Anti-Virus* statistics on the number of scripts scanned and blocked.

Web Anti-Virus guards HTTP traffic as follows:

1. Each web page or file that can be accessed by the user or by a certain application via HTTP is intercepted and analyzed by *Web Anti-Virus* for

malicious code. Malicious objects are detected using both the threat signatures included in Kaspersky Anti-Virus, and the heuristic algorithm. The signatures contain descriptions of all malicious programs known to date, and methods for neutralizing them. The heuristic algorithm can detect new viruses that have not yet been entered in the threat signatures.

2. After the analysis, you have the following available courses of action:
 - a. If the web page or object contains malicious code, the program blocks access to it, and a message appears on the screen, stating that the object or page is infected.
 - b. If the file or web page does not contain malicious code, the program immediately grants the web browser access to it.

Scripts are scanned according to the following algorithm:

1. Web Anti-Virus intercepts each script run on a web page and scans them for malicious code.
2. If a script contains malicious code, Web Anti-Virus blocks it and informs the user with a special popup notice.
3. If no malicious code is discovered in the script, it is run.

9.1. Selecting the web security level

Kaspersky Anti-Virus protects you while you use the Internet at one of the following levels (see Figure 29):

High – the level with the most comprehensive monitoring of scripts and objects incoming via HTTP. The program performs a thorough scan of all objects using the full set of threat signatures. This level of protection is recommended for sensitive environments, when no other HTTP security tools are being used.

Recommended – this level scans the same objects as **High**, but limits the caching time for file fragments, thus accelerating the scan and returning objects to the user sooner.

Low – the security level with settings that let you comfortably use resource-intensive applications, since the scope of objects scanned is reduced by using a limited set of . This security level is recommended if you have additional web protection software installed on your computer.

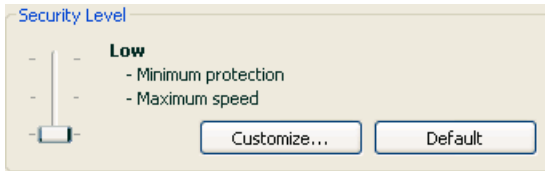


Figure 29. Selecting a web security level

By default, the protection level is set to **Recommended**.

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

To edit the security level:

Adjust the sliders. By altering the security level, you define the ratio of scan speed to the total number of objects scanned: the fewer objects are scanned for malicious code, the higher the scan speed.

If a preset level does not meet your needs, you can create a **Custom settings** security level. Let's look at an example of when such a level would be useful.

Example:

Your computer connects to the Internet via a modem. It is not on a corporate LAN, and you have no anti-virus protection for incoming HTTP traffic.

Due to the nature of your work, you regularly download large files from the Internet. Scanning files like these takes up, as a rule, a fair amount of time.

How do you optimally protect your computer from infection through HTTP traffic or a script?

Tip for selecting a level:

Judging from this basic information, we can conclude that your computer is running in a sensitive environment, and you are at high risk for infection through HTTP traffic, because there is no centralized web protection and due to the use of dial-up to connect to the Internet.

It is recommended that you use **High** as your starting point, with the following changes: you are advised to limit the caching time for file fragments during the scan.

To modify a preinstalled security level:

click the **Customize** button in the Web Anti-Virus settings window. Edit the web protection settings (see 9.2 on pg. 98) in the window that opens, and click **OK**.

9.2. Configuring Web Anti-Virus

Web Anti-Virus scans all objects that are loaded on your computer via HTTP and monitors any WSH scripts (JavaScript or Visual Basic Scripts, etc.) run.

You can configure Web Anti-Virus settings to increase component operation speed, specifically:

- Set the scanning algorithm by selecting a complete or limited set of threat signatures
- Creating a list of trusted web addresses

It is also possible to select the actions that Web Anti-Virus will take in response to discovering dangerous HTTP objects.

The following sections examine these settings in detail.

9.2.1. Setting a scan method

You can scan data from the Internet using one of the following algorithms:

- *Streaming scan* – this method for detecting malicious code in network traffic scans data on the fly: as a file is downloading from the Internet, Web Anti-Virus scans the file's portions as they are downloaded, which delivers the scanned object to the user more quickly. At the same time, a limited set of threat signatures is used to perform streaming scans (only the most active threats), which significantly lowers the security level for using the Internet.
- *Buffering scan* – this method scans objects only after they have been fully downloaded to the buffer. After the scan is complete, the program either passes the object to the user or blocks it.

When using this scan type, the full threat signature set is used, which improves the level of malicious code detection. However, using this algorithm increases object processing time, and hence makes web browsing slower: it can also cause problems when copying and processing large objects because the connection with the HTTP client can time out.

One way to solve this problem is to limit the caching time for object fragments downloaded from the Internet. When the time limit expires, the user will receive the downloaded part of the file without it being scanned, but once the object is fully copied, it will be scanned in its entirety. This can deliver the object to the user faster and solve the problem of interrupting the connection without reducing security while using the Internet.

To select the scanning algorithm that Web Anti-Virus will use:

1. Click on the **Customize** button in the Web Anti-Virus configuration window.
2. In the window that opens (see fig. 30), select the option you want in the **Scan method** section.

By default, Web Anti-Virus performs a buffered scan on Internet data, and uses the complete threat signature set. The default caching time for file fragments is one second.

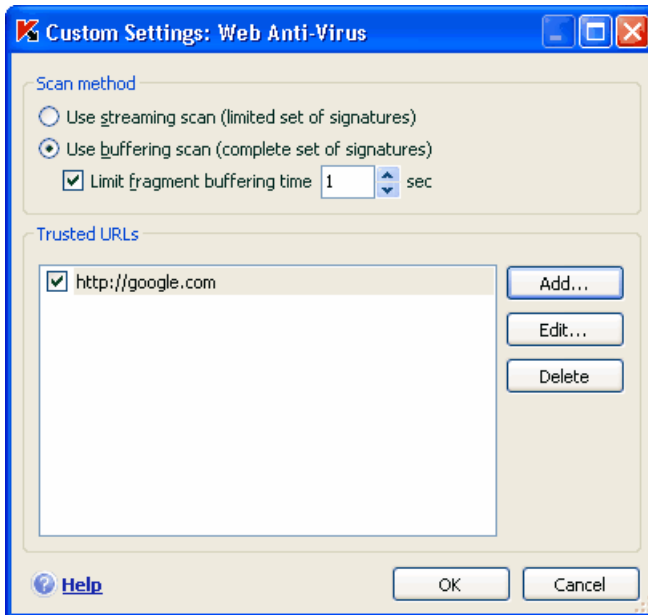


Figure 30. Configuring Web Anti-Virus

Warning!

If you encounter problems accessing resources like Internet radio, streaming video, or Internet conferencing, use streaming scan.

9.2.2. Creating a trusted address list

You have the option of creating a list of trusted addresses whose contents you fully trust. Web Anti-Virus will not analyze data from those addresses for dangerous objects. This feature can be used if Web Anti-Virus hinders downloading a certain file by blocking an attempt to download it.

To create a list of trusted addresses:

1. Click on the **Customize** button in the Web Anti-Virus configuration window.
2. In the window that opens (see fig. 30), create a list of trusted servers in the **Trusted URLs** section. To do so, use the buttons to the right of the list.

When entering a trusted address, you can create masks with the following wildcards:

* – any combination of characters.

Example: If you create the mask ***abc***, no URL contain **abc** will be scanned. For example: www.virus.com/download_virus/page_0-9abcdef.html

? – any single character.

Example: If you create mask **Patch_123?.com**, URLs containing that series of characters plus any single character following the 3 will not be scanned. For example: **Patch_1234.com** However, **patch_12345.com** will be scanned.

If an * or ? is part of an actual URL added to the list, when you enter them, you must use a backslash to override the * or ? following it.

Example: You want to add this following URL to the trusted address list: www.virus.com/download_virus/virus.dll?virus_name=

For Kaspersky Anti-Virus not to process ? as a wildcard, put a backslash (\) in front of it. Then the URL that you are adding to the exclusion list will be as follows: www.virus.com/download_virus/virus.dll?virus_name=

9.2.3. Restoring default Web Anti-Virus settings

When configuring Web Anti-Virus, you can always return to the default performance settings, which Kaspersky Lab considers to be optimal and has combined as the **Recommended** security level.

To restore the default Web Anti-Virus settings:

1. Select **Web Anti-Virus** in the main window and go to the component settings window by clicking [Settings](#).
2. Click the **Default** button in the **Security Level** section.

9.2.4. Selecting responses to dangerous objects

If analyzing an HTTP object shows that it contains malicious code, the Web Anti-Virus response depends on the actions you select.

To configure Web Anti-Virus reactions to detecting a dangerous object:

Open the Kaspersky Anti-Virus settings window and select **Web Anti-Virus**. The possible responses for dangerous objects are listed in the **Action** section (see fig. 31).

By default, when a dangerous HTTP object is detected, Web Anti-Virus displays a warning on the screen and offers a choice of several actions for the object.

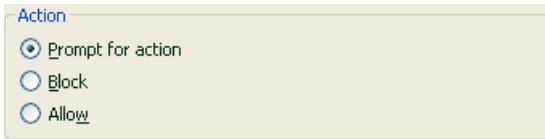


Figure 31. Selecting actions for dangerous scripts

The possible options for processing dangerous HTTP objects are as follows.

| If the action selected was | If a dangerous object is detected in the HTTP traffic |
|---|--|
| <input checked="" type="radio"/> Prompt for action | Web Anti-Virus will issue a warning message containing information about what malicious code has potentially infected the object, and will give you a choice of responses. |
| <input type="radio"/> Block | Web Anti-Virus will block access to the object and will display a message on screen about blocking it. Similar information will be recorded in the report (see 14.3 on pg. 158). |
| <input type="radio"/> Allow | Web Anti-Virus will grant access to the object. This information is logged in the report. |

Web Anti-Virus always blocks dangerous scripts, and issues popup messages that inform the user of the action taken. You cannot change the response to dangerous scripts, other than by disabling the script scanning module.

CHAPTER 10. PROACTIVE DEFENSE

Warning!

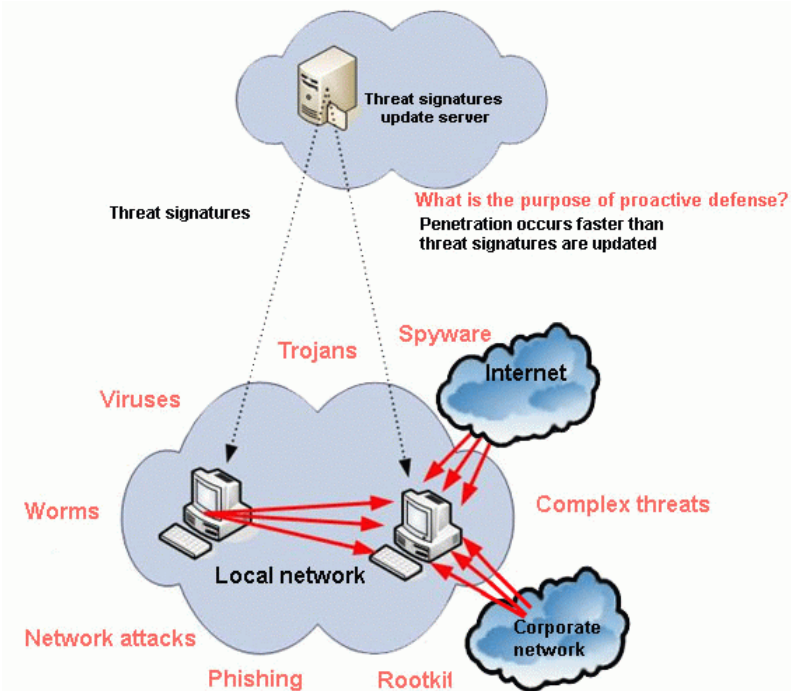
This version of the application does not have the proactive defense component: There are no Proactive Defense components in this version of the application (**Application Integrity Control** and **Office Guard**) for computers running Microsoft Windows XP Professional x64 Edition or computers running Microsoft Windows Vista or Microsoft Windows Vista x64.

Kaspersky Anti-Virus protects you both from known threats and from new ones about which there is no information in the . This is ensured by a specially developed component – *Proactive Defense*.

The need for Proactive Defense has grown as malicious programs have begun to spread faster than anti-virus updates can be released to neutralize them.

The reactive technique, on which anti-virus protection is based, requires that a new threat infect at least one computer, and requires enough time to analyze the malicious code, add it to the threat signatures and update the database on user computers. By that time, the new threat might have inflicted massive damages.

The preventative technologies provided by Kaspersky Anti-Virus Proactive Defense do not require as much time as the reactive technique, and neutralize new threats before they harm your computer. How is this done? In contrast with reactive technologies, which analyze code using a threat signature database, preventative technologies recognize a new threat on your computer by the sequence of actions executed by a certain program. The application installation includes a set of criteria that can help determine how dangerous the activity of one program or another is. If the activity analysis shows that a certain program's actions are suspicious, Kaspersky Anti-Virus will take the action assigned by the rule for activity of the specific type.



Dangerous activity is determined by overall program behavior. For example, when actions are detected such as a program copying itself to network resources, the startup folder, or the system registry, and then sending copies of itself, it is highly likely that this program is a worm. Dangerous behavior also includes:

- Changes to the file system
- Modules being embedded in other processes
- Masking processes in the system
- Modification of certain Microsoft Window system registry keys

Proactive Defense tracks and blocks all dangerous operations. Proactive Defense also tracks all macros executed in Microsoft Office applications.

Proactive Defense uses a set of rules included with the application, as well as user-defined rules created while using the application. A *Rule* is a set of criteria that defines suspicious behavior and how Kaspersky Anti-Virus reacts to it.

Individual rules are provided for application activity and monitoring changes to the system registry, macros, and programs run on the computer. You can alter

the rules at your own discretion by adding, deleting, or editing them. Rules can block actions or grant permissions.

Let's examine the Proactive Defense algorithms:

1. Immediately after the computer is started, Proactive Defense analyzes the following factors, using the set of rules and exclusions:
 - *Actions of each application running on the computer.* Proactive Defense records a history of actions taken in order and compares them with sequences characteristic of dangerous activity (a database of dangerous activity types comes with the program and is updated with the threat signatures).
 - *Actions of each VBA macro run* are analyzed for signs of malicious activity.
 - *Integrity of the program modules* of the programs installed on your computer, which detects the replacement of program modules by versions with malicious code injected into them.
 - *Each attempt to edit the system registry* by deleting or adding system registry keys, entering values for keys in an inadmissible format that prevents them from being viewed or edited, etc.).
2. The analysis is conducted using allow and block rules from Proactive Defense.
3. After the analysis, the following courses of action are available:
 - If the activity satisfies the conditions of the Proactive Defense allow rule or does not match any of the block rules, it is not blocked.
 - If the activity is ruled as dangerous on the basis of the relevant criteria, the next steps taken by the component match the instructions specified in the rule: usually the activity is blocked. A message will be displayed on the screen specifying the dangerous program, its activity type, and a history of actions taken. You must accept the decision, block, or allow this activity on your own. You can create a rule for the activity and cancel the actions taken in the system.

10.1. Proactive Defense settings

The categories of settings (see fig. 32) for the Proactive Defense component are as follows:

- *Whether application activity is monitored on your computer*

This Proactive Defense feature is enabled by checking the box **Enable Application Activity Analyzer**. By default this mode is enabled, which ensures that the actions of any programs opened on your computer will be closely tracked and compared to a configurable list of dangerous activities. You can configure the order in which applications are processed (see 10.1.1 on pg. 106) for that activity. You can also create Proactive Defense exclusions, which will stop the monitoring of selected applications.

- *Whether Application Integrity Control is enabled*

This feature is responsible for the integrity of application modules (dynamic link libraries, or DLLs) installed on your computer, and is enabled by checking the box **Application Integrity Control** box. Integrity is tracked by monitoring the checksum of the program modules and of the program itself. You can create integrity control rules for the modules of any application. To do so, you must add the application to the monitored applications list.

This Proactive Defense component is not available under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64.

- *Whether system registry changes are monitored*

By default, **Enable Registry Guard** is checked, which means Kaspersky Anti-Virus analyzes all attempts to make changes to the Windows system registry keys.

You can create your own rules (see 10.1.4.2 on pg. 119) for monitoring the registry, depending on the Microsoft Windows registry key.

- *Whether macros are scanned*

The monitoring of Visual Basic for Applications macros on your computer is controlled by checking the box **Enable Office Guard**, which is checked by default.

You can select which macros are considered dangerous and what to do to them (see 10.1.3 on pg. 114).

This Proactive Defense component is not available under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64.

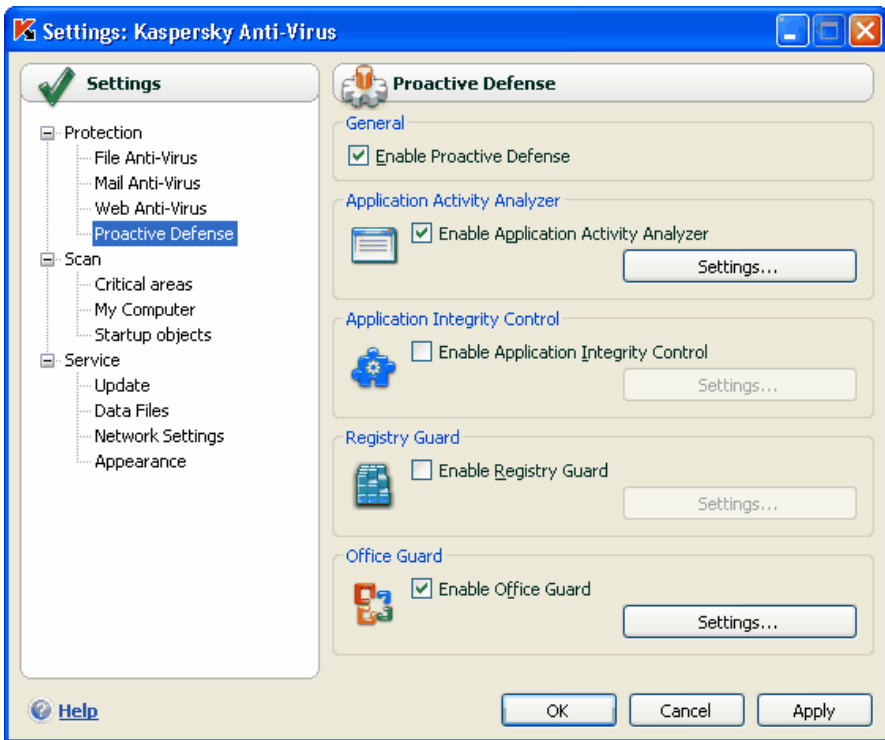


Figure 32. Proactive Defense settings

You can configure exclusions (see 6.3.1 on pg. 60) for Proactive Defense modules and create a trusted application list (see 6.3.2 on pg. 65).

The following sections examine these aspects in more detail.

10.1.1. Activity control rules

Note that configuring application control under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista or Microsoft Windows Vista x64 differs from the configuration process on other operating systems. Information about configuring activity control for these operating systems is provided at the end of this section.

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

Select the **Enable Application Activity Analyzer** checkbox if you want to monitor the activity of applications.

Let's take a look at several types of events that occur in the system that the application will track as suspicious:

- *Dangerous activity (behavior analysis)*. Kaspersky Anti-Virus analyzes the activity of applications installed on your computer, and based on the list of rules created by Kaspersky Lab, detects dangerous or suspicious actions by the programs. Such actions include, for example, masked program installation, or programs copying themselves.
- *Open browser with settings*. By analyzing this type of activity, you can detect attempts to open a browser with settings. This activity is characteristic of opening a web browser from an application with certain command prompt settings: for example, when you click a link to a certain URL in an advertisement e-mail.
- *Intrusion into process* – adding executable code or creating an additional stream to the process of a certain program. This activity is widely used by Trojans.
- *Appearance of masked processes (Rootkit)*. A rootkit is a set of programs used to mask malicious programs and their processes in the system. Kaspersky Anti-Virus analyzes the operating system for masked processes.
- *Invaders*. This activity is used in attempts to read passwords and other confidential information displayed in operating system dialog boxes. Kaspersky Anti-Virus traces this activity if attempts are made to intercept data transferred between the operating system and the dialog box.
- *Suspicious characters in the registry*. The system registry is a database for storing system and user settings that control the operation of Windows, as well as any utilities established on the computer. Malicious programs, attempting to mask their presence in the system, copy incorrect values in registry keys. Kaspersky Anti-Virus analyzes system registry entries for suspicious values.
- *Suspicious activity in the system*. The program analyzes actions executed by Microsoft Windows and detects suspicious activity. An example of suspicious activity would be an integrity breach, which involves modifying one or several modules in a monitored application since the time it was last run.

- *Keyloggers*. This activity is used in attempts by malicious programs to read passwords and other confidential information which you have entered using your keyboard.
- *Windows Task Manager protection*. Kaspersky Anti-Virus protects Task Manager from malicious modules injecting themselves into it when aimed at blocking Task Manager operation.

The list of dangerous activities can be extended automatically by the Kaspersky Anti-Virus update process, but it cannot be edited by the user. You can:

- Turn off monitoring for an activity by deselecting the next to its name
- Edit the rule that Proactive Defense uses when it detects a dangerous activity
- Create an exclusion list (see 6.3 on pg. 59) by listing applications that you do not consider dangerous.

To configure activity monitoring,

1. Open the Kaspersky Anti-Virus settings window by clicking Settings in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Application Activity Analyzer** section.

The types of activity that Proactive Defense monitors are listed in the **Settings: Application Activity Analyzer** window (see fig. 33).

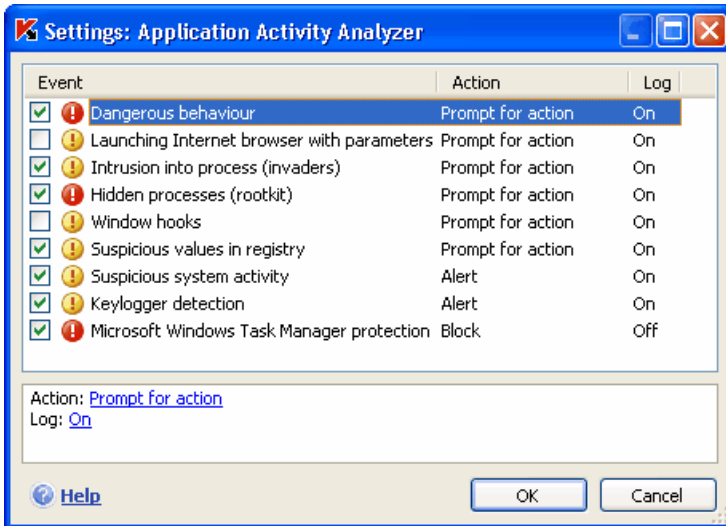


Figure 33. Configuring application activity control

To edit a dangerous activity monitoring rule, select it from the list and assign the rule settings in the lower part of the tab:

- Assign the Proactive Defense response to the dangerous activity.
- You can assign any of the following actions as a response: [allow](#), [prompt for action](#), and [terminate process](#). Left-click on the action link until it reaches the value you require. In addition to stopping the process, you can place the application that initiated the dangerous activity in Quarantine. To do so, use the [On](#) / [Off](#) link across from the appropriate setting. You can assign a time value for how frequently the scan will run for detecting hidden processes in the system.
- Choose if you want to generate a report on the operation carried out. To do so, click on the **Log** link until it shows [On](#) or [Off](#) as required.

To turn off monitoring for a dangerous activity, uncheck the next to the name in the list.

Specifics of configuring application activity control in Kaspersky Anti-Virus under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64:

If you are running one of the operating systems listed above, only one type of system event is controlled, dangerous activity (behavior analysis) . If you want Kaspersky Anti-Virus to monitor modifications of system user accounts in

addition to dangerous activity, selected the **Watch system user accounts** checkbox (see 34).

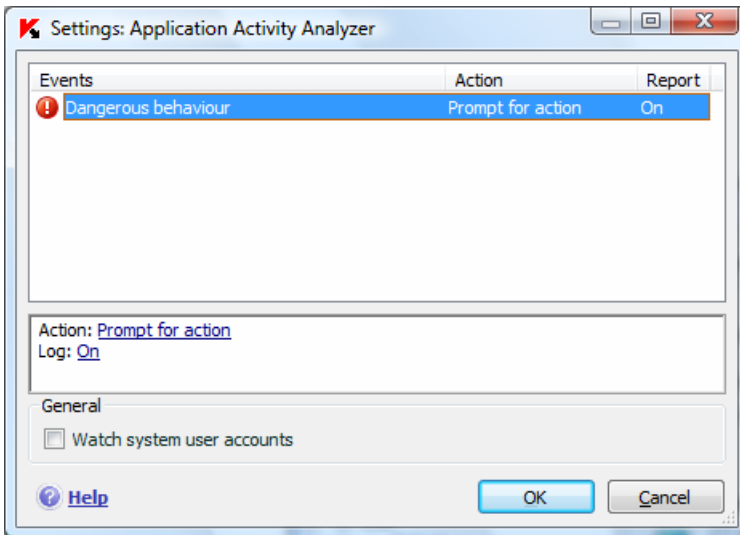


Figure 34. Configuring application integrity control in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.1.2. Application Integrity Control

This Proactive Defense component does not work under Microsoft Windows XP Professional x64 Edition, or Microsoft Windows Vista or Microsoft Windows Vista x64.

There are a number of programs that are critical for the system that could be used by malicious programs to distribute themselves, such as browsers, mail clients, etc. As a rule, these are system applications and processes used for accessing the Internet, working with email and other documents. It is for this reason that these applications are considered *critical* in activity control.

Proactive Defense monitors these critical applications closely, analyzing their activity and observing other processes which they spawn. Kaspersky Anti-Virus comes with a list of critical applications and a monitoring rule has been created for each of them that controls application activity. You can extend this list of critical applications, and delete or edit the rules for the applications on the list provided.

Besides the list of critical applications, there is a set of trusted modules allowed to be opened in all controlled applications. For example, modules which are digitally signed by the Microsoft Corporation. It is highly unlikely that these modules would be malicious, so it is not necessary to monitor them closely, which in turn lightens the load on your computer when using Proactive Defense.

Components with Microsoft-signed signatures are automatically designated as trusted applications. If necessary, you can add or delete components from the list.

The monitoring of processes and their integrity in the system is enabled by checking the box **Enable Application Integrity Control** in the Proactive Defense settings window: by default, the box is unchecked. If you enable this feature, each application or application module opened is checked against the critical and trusted applications list. If the application is on the list of critical applications, its activity is controlled by Proactive Defense in accordance with the rule created for it.

To configure Application Integrity Control:

1. Open the Kaspersky Anti-Virus settings window by clicking Settings in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Application Integrity Control** box.

Let's examine working with critical and trusted processes in greater detail.

10.1.2.1. Configuring Application Integrity Control rules

Critical applications are executable files of programs which are extremely important to monitor, since malicious files use such programs to distribute themselves.

A list of critical application was created when the application was installed, and is shown on the **Critical applications** tab (see fig. 35): each application has its own monitoring rule to regulate its behavior. You can edit existing rules and create your own.

Proactive Defense analyzes the following operations involving critical applications: their launch, changing the makeup of application modules, and starting an application as a child process. You can select the Proactive Defense response to each of the operations listed (allow or block the operation), and also specify whether to log component activity in the component report. The default settings allow most critical operations are allowed to start, be edited, or be started as child processes.

To add an application to the critical application list and create a rule for it:

1. Click **Add** on the **Critical applications** tab. A context menu will open: click **Browse** to open the standard file selection window, or click **Applications** to see a list of currently active applications and select one of them as necessary. The new application will be added to the top of the list, and **allow** rules (i.e. all activities are allowed) will be created for it by default. When that application is first started, the modules that it accesses will be added to the list, and those modules will similarly be given **allow** rules.

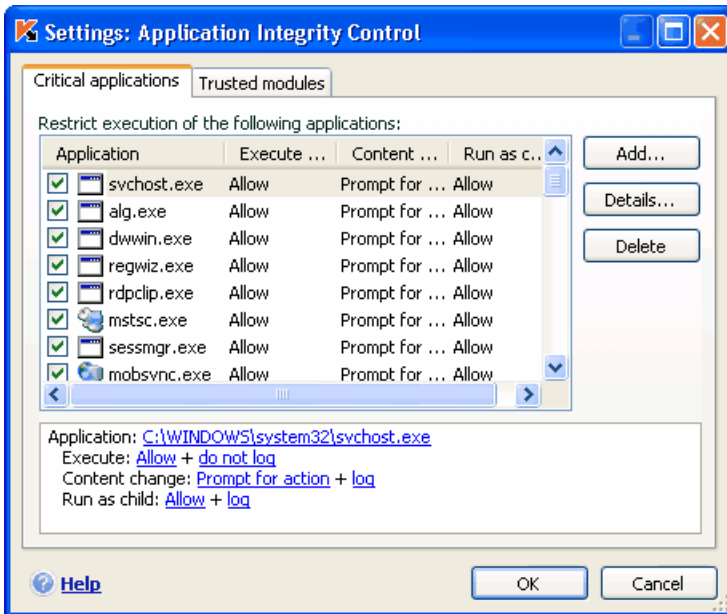


Figure 35. Configuring Application Integrity Control

2. Select a rule on the list and assign rule settings in the lower portion of the tab:
 - Define the Proactive Defense response to attempts to execute the critical application, change its makeup, or start it as a child process.

You can use any of these actions as a response: [allow](#), [prompt for action](#), or [block](#). Left-click on the action link until it reaches the value that you need.

- Choose if you want to generate a report about the activity, by clicking log / do not log.

To turn off the monitoring of an application's activity, uncheck the next to its name.

Use the **Details** button to view a detailed list of modules for the application selected. The **Settings: application modules** window contains a list of the modules that are used when a monitored application is started and make up the application. You can complete and edit the list using the **Add** and **Delete** buttons in the right-hand portion of the window.

You can also allow any controlled application modules to load or block them. By default, an allow rule is created for each module. To modify the action, select the module from the list and click the **Modify** button. Select the needed action in the window that opens.

Note that Kaspersky Anti-Virus trains the first time you run the controlled application after installing Kaspersky Anti-Virus until you close that application. The training process produces a list of modules used by the application. Integrity Control rules will be applied the next time you run the application.

10.1.2.2. Creating a list of shared components

Kaspersky Anti-Virus includes a list of components which can be opened by all controlled applications. You will find this list on the **Trusted modules** tab (see fig. 36). It includes modules used by Kaspersky Anti-Virus, Microsoft-signed components: components can be added or removed by the user.

If you install programs on your computer, you can ensure that those with modules signed by Microsoft are automatically added to the trusted modules list. To do this, check **Automatically add components signed by Microsoft Corporation to this list**. Then if a controlled application attempts to open the Microsoft-signed module, Proactive Defense will automatically allow the module to load without checking, and add it to the list of shared components.

To add to the trusted module list, click **Add** and in the standard file selection window, and select the module.

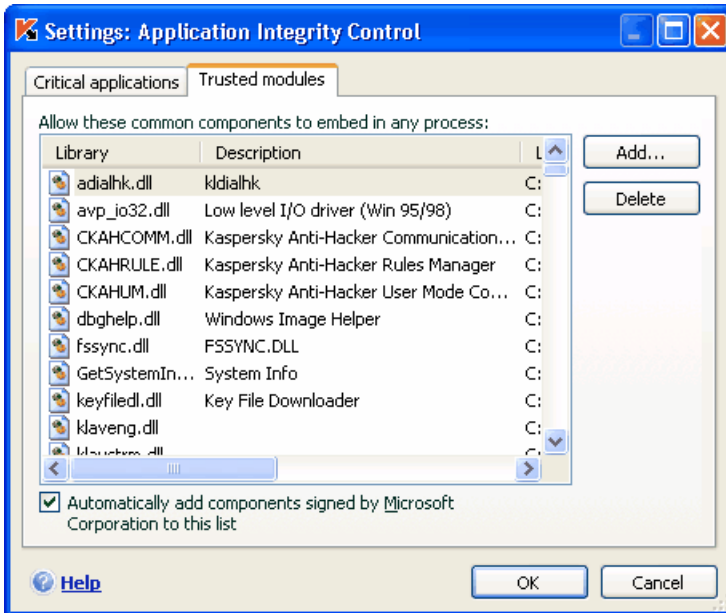


Figure 36. Configuring the trusted module list

10.1.3. Office Guard

This Proactive Defense component does not work under Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64.

You can enable scanning and processing of dangerous macros run on your computer by checking **Enable Office Guard** (see fig. 32). The checkbox is selected by default, and the activity of each macro run is traced for dangerous behavior. If suspicious activity is detected, Proactive Defense allows or blocks the macro.

Example:

The macro *PDFMaker* is a plug-in for the Adobe Acrobat toolbar in Microsoft Office Word that can create a .pdf file out of any document. Proactive Defense classifies embedding elements in software as a dangerous action. If Office Guard is enabled, when a macro is loaded Proactive Defense issues a warning on the screen, informing you that it has detected a dangerous macro command. You can choose to terminate that macro or allow it to continue.

You can configure Kaspersky Anti-Virus's reactions to macros executing suspicious behavior. If you are sure that this macro is not dangerous when working with a specific file, for example, a Microsoft Word document, we recommend creating an exclusion rule. If a situation occurs that matches the terms of the exclusion rule, the suspicious action performed by the macro will not be processed by Proactive Defense.

To configure Office Guard:

1. Open the Kaspersky Anti-Virus settings window by clicking Settings in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Office Guard** box.

Rules for processing dangerous macros are configured in the **Office Guard settings** window (see fig. 37) It contains default rules for behavior that Kaspersky Lab classifies as dangerous. The actions of dangerous macros include, for example, embedding modules in programs and deleting files.

If you do not consider a behavior on the list to be dangerous, uncheck the box next to its name. For example, you might frequently use macros to open files (not as read-only) and you are positive that this operation is not malicious.

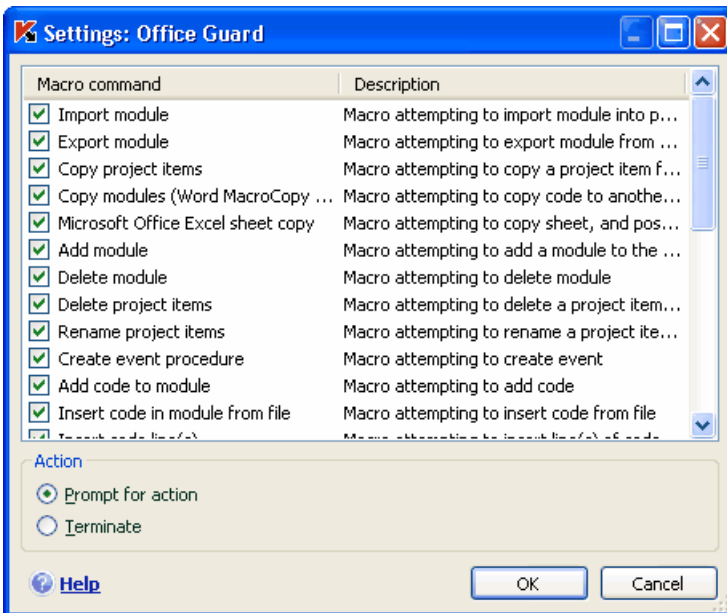


Figure 37. Configuring Office Guard settings

For Kaspersky Anti-Virus not to block the macro:

uncheck the box next to that action. The program will no longer consider that behavior dangerous and Proactive Defense will not process it.

By default, whenever the program detects an action initiated by a macro on your computer, the application will ask you if you want to allow or block that macro.

In order for the program to automatically block all dangerous behavior without prompting the user:

In the window with the macro list, select  **Terminate**.

10.1.4. Registry Guard

One of the goals of many malicious programs is to edit the Windows system registry on your computer. These can either be harmless jokes, or more malicious programs that present a serious threat to your computer.

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

A special Proactive Defense module can detect unknown threats that attempt to edit registry keys on your computer. You can enable it by checking the box **Enable Registry Guard** in the **Proactive Defense** settings window.

To configure system registry monitoring:

1. Open the Kaspersky Anti-Virus settings window by clicking **Settings** in the main program window.
2. Select **Proactive Defense** in the settings tree.
3. Click the **Settings** button in the **Registry Guard** section.

Kaspersky Lab has created a list of rules that control registry file operations, and have included it in the program. Operations with registry files are categorised into logical groups such as *System Security*, *Internet Security*, etc. Each such group lists system registry files and rules for working with them. This list is updated when the rest of the application is updated.

The **Registry Guard** settings window (see fig. 38) displays the complete list of rules.

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

You can stop using any group of rules in the following ways:

- Uncheck the box next to the group's name. Then the group of rules will remain on the list but will not be used.
- Delete the group of rules from the list. We do not recommend deleting the groups created by Kaspersky Lab, since they contain a list of system registry files most often used by malicious programs.

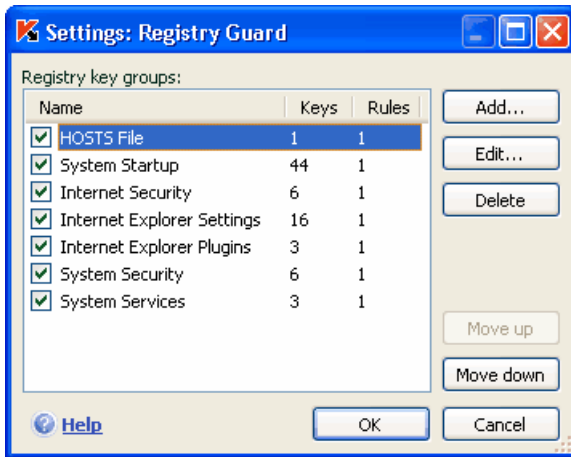


Figure 38. Controlled registry key groups

You can create your own groups of monitored system registry files. To do so, click **Add** in the file group window.

Take these steps in the window that opens:

1. Enter the name of the new registry key group for monitoring system registry keys in the **Name** field.
2. Select the **Keys** tab, and create a list of system registry keys that will be included in the monitored group (see 10.1.4.1 on pg. 118) for which you want to create rules. This could be one or several keys.
3. Select the **Rules** tab, and create a rule for files (see 10.1.4.2 on pg. 119) that will apply to the keys selected on the Keys tab. You can create several rules and set the order in which they are applied.

10.1.4.1. Selecting registry keys for creating a rule

The file group created should contain at least one system registry file. The **Keys** tab shows the list of files to which the rule(s) apply.

To add a system registry file:

1. Click on the **Add** button in the **Edit group** window (see fig. 39).
2. In the window that opens, select the registry file, or folder of files, for which you want to create the monitoring rule.
3. Specify the file value, or a mask for the group of files, to which you want the rule to apply in the **Value** field.
4. Check **Include subkeys** for the rule to apply to all files attached to the listed registry file.

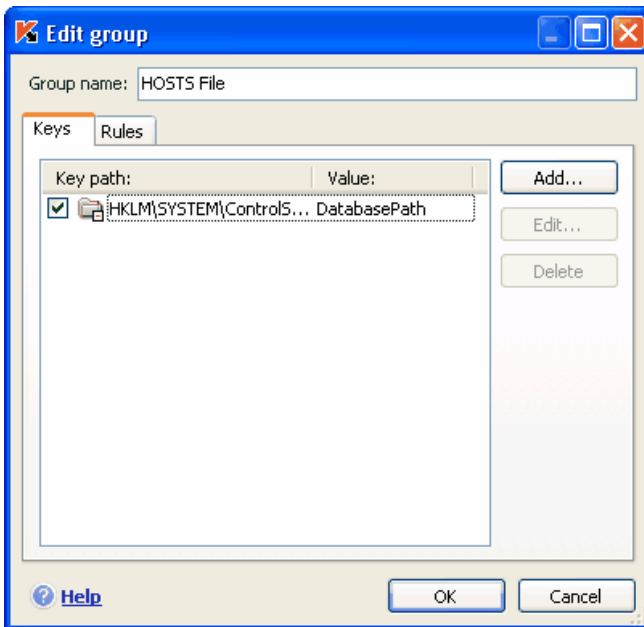


Figure 39. Adding controlled registry keys

You only need to use masks with an asterisk and a question mark at the same time as the **Include subkeys** feature if the wildcards are used in the name of the key.

If you select a folder of registry files using a mask and specify a specific value for it, the rule will be applied to that value for any key in the group selected.

10.1.4.2. Creating a Registry Guard rule

A Registry Guard rule specifies:

- The program whose access to the system registry is being monitored
- Proactive Defense's response when a program attempts to execute an operation with a system registry files

To create a rule for your selected system registry files:

1. Click **New** on the **Rules** tab. The new rule will be added at the top of the list (see fig. 40).

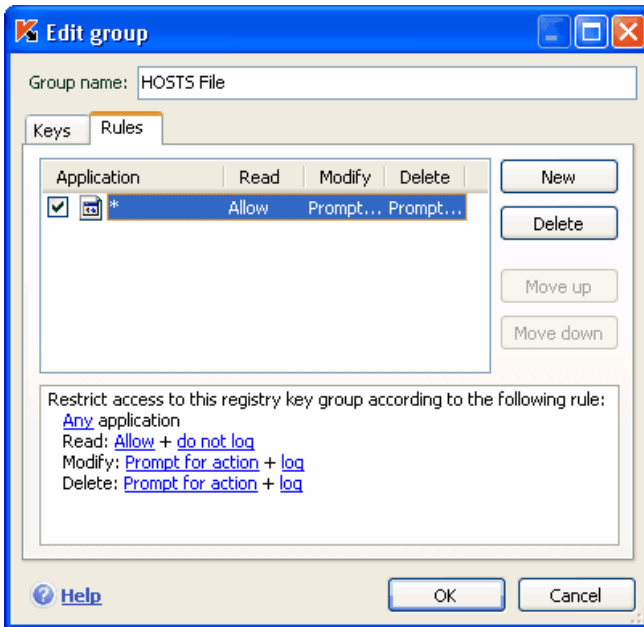


Figure 40. Creating an registry key monitoring rule

2. Select a rule on the list and assign the rule settings in the lower portion of the tab:
 - Specify the application.

The rule is created for any application by default. If you want the rule to apply to a specific application, left-click on [any](#) and it will change to [this](#). Then click on the [specify application name](#) link. A context menu will open: click **Browse** to see the standard file selection window, or click **Applications** to see a list of open applications, and select one of them as necessary.

- Define the Proactive Defense response to the selected application attempting to read, edit, or delete system registry files.

You can use any of these actions as a response: [allow](#), [prompt for action](#), and [block](#). Left-click on the link with the action until it reaches the value that you need.

- Choose if you want to generate a report on the operation carried out, by clicking on the [log / do not log](#) link.

You can create several rules, and order their priority using the **Move Up** and **Move Down** buttons. The higher the rule is on the list, the higher the priority assigned to it will be.

You can also create an *allow* rule (i.e. all actions are allowed) for a system registry file from a notification window stating that a program is trying to execute an operation with the file. To do so, click [Create allow rule](#) in the notice and select what the rule will apply to in the window that opens.

CHAPTER 11. SCANNING FOR VIRUSES ON YOUR COMPUTER

One of the important aspects of protecting your computer is scanning user-defined areas for viruses. Kaspersky Anti-Virus can scan individual items – files, folders, disks, plug-and-play devices – or the entire computer. Scanning for viruses stops malicious code which has gone undetected by real-time protection components from spreading.

Kaspersky Anti-Virus includes three default scan tasks:

Critical Areas

Scans all critical areas of the computer for viruses, including: system memory, programs loaded on startup, boot sectors on the hard drive, and the *Windows* and *system32* system directories. The task aims to detect active viruses quickly on the system without fully scanning the computer.

My Computer

Scans for viruses on your computer with a thorough inspection of all disk drives, memory, and files.

Startup Objects

Scans for viruses all programs loaded when the operating system boots.

The default settings for these tasks are the recommended ones. You can edit these settings (see 11.4.4 on pg. 129) or create a schedule (see 6.5 on pg. 69) for running tasks.

You also have the option of creating your own tasks (see 11.4.3 on pg. 129) and creating a schedule for them. For example, you can schedule a scan task for email databases once per week, or a virus scan task for the **My Documents** folder.

In addition, you can scan any object for viruses (for example, a portable hard drive used for transferring files between office and home) without creating a special scan task. You can select an object to scan from the Kaspersky Anti-Virus interface, or with the standard tools of the Windows operating system (for example, in the **Explorer** program window or on your **Desktop**).

You can view a complete list of virus scan tasks for your computer by clicking on **Scan** in the left-hand pane of the main application window.

11.1. Managing virus scan tasks

You can run a virus scan task manually or automatically using a schedule (see 6.5 on pg. 69).

To start a virus scan task manually:

Check the box beside the task name in the **Scan** section of the main program window, and click the ► button on the status bar.

The tasks currently being performed are displayed in the context menu by right-clicking on the system tray icon.

To pause a task:

Click the || button on the status bar. The task status will change to *paused*. This will pause the scan until you start the task again manually or it starts again automatically according to the schedule.

To stop a task:

Click the ■ button on the status bar. The task status will change to *stopped*. This will stop the scan until you start the task again manually or it starts again automatically according to the schedule. The next time you run the task, the program will ask if you would like to continue the task where it stopped or begin it over.

11.2. Creating a list of objects to scan

To view a list of objects to be scanned for a particular task, select the task name (for example, **My computer**) in the **Scan** section of main program window. The list of objects will be displayed in the right-hand part of the window under the status bar (see fig. 41).

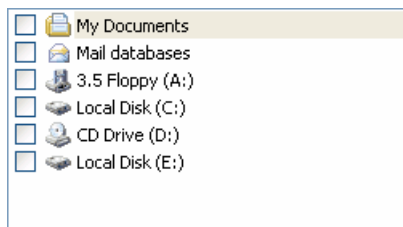


Figure 41. List of objects to scan

Object scan lists are already made for default tasks created when you install the program. When you create your own tasks or select an object for a virus scan task, you can create a list of objects.

You can add to or edit an object scan list using the buttons to the right of the list. To add a new scan object to the list, click the **Add** button, and in the window that opens select the object to be scanned.

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

In addition, when you add a folder that contains embedded objects to a scan area, you can edit the recursion. To do so, use the corresponding item on the context menu.

To delete an object, select it from the list (when you do so, the name of the object will be highlighted in gray) and click the **Delete** button. You can temporarily disable scanning for individual objects for any task without deleting them from the list. To do so, uncheck the box beside the object that you do not want scanned.

To start a scan task, click the **Scan** button, or select **Start** from the menu that opens when you click the **Actions** button.

In addition, you can select an object to be scanned with the standard tools of the Windows operating system (for example, in the Explorer program window or on your Desktop, etc.) (see fig. 42). To do so, select the object, open the Windows context menu by right-clicking, and select **Scan for Viruses**.

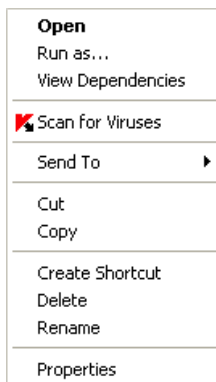


Figure 42. Scanning objects from the Windows context menu

11.3. Creating virus scan tasks

To scan objects on your computer for viruses, you can use built-in scan tasks included with the program and create your own tasks. New scan tasks are created using existing tasks that a template.

To create a new virus scan task:

1. Select the task with the settings closest to those you need, in the **Scan** section of the main program window.
2. Open the context menu by right-clicking on the task name, or click the **Actions** button to the right of the scan object list, and select **Save as....**
3. Enter the name for the new task in the window that opens and click **OK**. A task with that name will then appear in the list of tasks in the **Scan** section of the main program window.

Warning!

There is a limit to the number of tasks that the user can create. The maximum is four tasks.

The new task is a copy of the one it was based on. You need to continue setting it up by creating an scan object list (see 11.4.2 on pg. 126), setting up properties that govern the task (see 11.4.4 on pg. 129), and, if necessary, configuring a schedule (see 6.5 on pg. 69) for running the task automatically.

To rename a task:

Select the task in the **Scan** section of the main program window. Right-click on the task's name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Rename**.

Enter the new name for the task in the window that opens and click **OK**. The task name will also be changed in the **Scan** section.

To delete a task:

Select the task in the **Scan** section of the main program window. Right-click on the task's name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Delete**.

You will be asked to confirm that that you want to delete the task. The task will then be deleted from the list of tasks in the **Scan** section.

Warning!

You can only rename and delete tasks that you have created.

11.4. Configuring virus scan tasks

The methods are used to scan objects on your computer are determined by the properties assigned for each task.

To configure task settings:

Select the task name in the **Scan** of the main window. Right-click on the task name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Settings**.

You can use the settings window for each task to:

- Select the security level that the task will use (see 11.4.1 on pg. 125)
- Edit advanced settings:
 - define what file types are to be scanned for viruses (see 11.4.2 on pg. 126)
 - configure task start using a different user profile (see 6.4 on pg. 68)
 - configure advanced scan settings (see 11.4.5 on pg. 131)
- restore default scan settings (see 11.4.3 on pg. 129)
- select an action that the program will apply when it detects an infected or suspicious object (see 11.4.4 on pg. 129)
- create a schedule (see 6.5 on pg. 69) to automatically run tasks.

In addition, you can configure global settings (see 11.4.6 on pg. 133) for running all tasks.

The following sections examine the task settings listed above in detail.

11.4.1. Selecting a security level

Each virus scan task can be assigned a security level (see fig. 43):

High – the most complete scan of the entire computer or individual disks, folders, or files. You are advised to use this level if you suspect that a virus has infected your computer.

Recommended – Kaspersky Lab experts recommend this level. The same files will be scanned as for the **High** setting, except for email databases.

Low – level with settings that let you comfortably use resource-intensive applications, since the scope of files scanned is reduced.

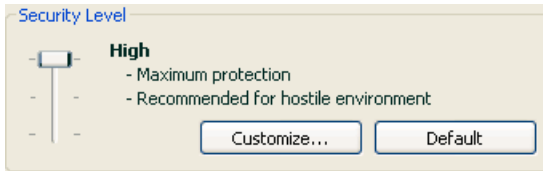


Figure 43. Selecting a virus scan security level

By default, the File Anti-Virus security level is set to **Recommended**.

You can raise or lower the scan security level by selecting the level you want or changing the settings for the current level.

To edit the security level:

Adjust the sliders. By adjusting the security level, you define the ratio of scan speed to the total number of files scanned: the fewer files are scanned for viruses, the higher the scan speed.

If none of the file security levels listed meet your needs, you can customize the protection settings. To do so, select the level that is closest to what you need as a starting point and edit its settings. If you do so, the level will be renamed as **Custom settings**.

To modify the settings for a security level:

click the **Settings** button in the task settings window. Edit the scan settings in the window that opens and click **OK**.

As a result, a fourth security level will be created, **Custom settings**, which contains the protection settings that you configured.

11.4.2. Specifying the types of objects to scan

By specifying the types of objects to scan, you establish which file formats, files sizes, and drives will be scanned for viruses when this task runs.

The file types scanned are defined in the **File types** section (see fig. 44). Select one of the three options:

- ① **Scan all files.** With this option, all objects will be scanned without exception.
- ② **Scan programs and documents (by content).** If you select this group of programs, only potentially infected files will be scanned – files into which a virus could imbed itself.

Note:

There are files in which viruses cannot insert themselves, since the contents of such files does not contain anything for the virus to hook onto. An example would be .txt files.

And vice versa, there are file formats that contain or can contain executable code. Examples would be the formats .exe, .dll, or .doc. The risk of insertion and activation of malicious code in such files is fairly high.

Before searching for viruses in an object, its internal header is analyzed for the file format (txt, doc, exe, etc.).

- ④ **Scan programs and documents (by extension).** In this case, the program will only scan potentially infected files, and in doing so, the file format will be determined by the filename's extension. Using the link, you can review a [list of file extensions](#) that are scanned with this option (see A.1 on pg. 206).

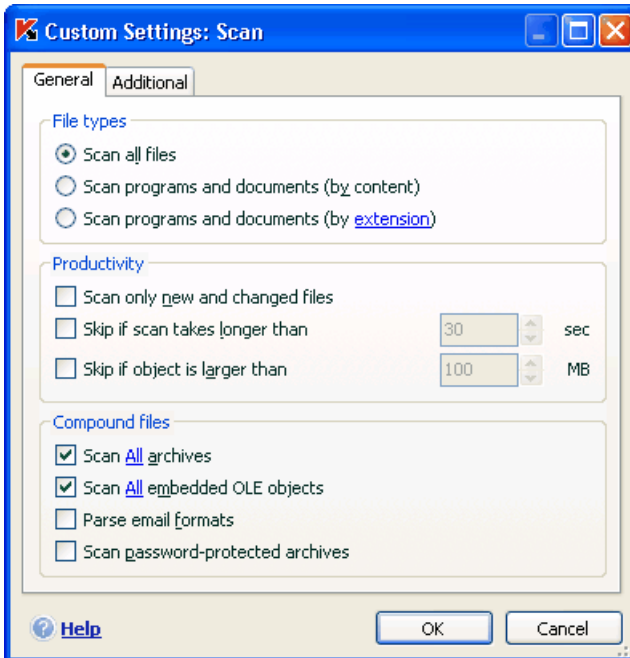


Figure 44. Configuring scan settings

Tip:

Do not forget that someone could send a virus to your computer with the extension .txt that is actually an executable file renamed as a .txt file. If you select the **Scan programs and documents (by extension)** option, the scan would skip such a file. If the **Scan programs and documents (by contents)** is selected, the program will analyze file headers, discover that the file is an .exe file, and thoroughly scan it for viruses.

In the **Productivity** section, you can specify that only new files and those that have been modified since the previous scan or new files should be scanned for viruses. This mode noticeably reduces scan time and increases the program's performance speed. To do so, you must check **Scan only new and changed files**. This mode extends to simple and compound files.

You can also set time and file size limits for scanning in the **Productivity** section.

Skip if scan takes longer than... secs. Check this option and enter the maximum scan time for an object. If this time is exceeded, this object will be removed from the scan queue.

Skip if object is larger than...MB. Check this option and enter the maximum size for an object. If this size is exceeded, this object will be removed from the scan queue.

In the **Compound files** section, specify which compound files will be analyzed for viruses:

Scan All/New Only archives – scan .rar, .arj, .zip, .cab, .lha, .jar, and .ice archives.

Warning!

Kaspersky Anti-Virus does not delete compressed file formats that it does not support (for example, .ha, .uue, .tar) automatically, even if you select the option of automatically curing or deleting if the objects cannot be cured.

To delete such compressed files, click the [Delete archives](#) link in the dangerous object detection notification. This notification will be displayed on the screen after the program begins processing objects detected during the scan. You can also delete infected archives manually.

Scan All/New Only embedded OLE objects– scan objects imbedded in files (for example, Excel spreadsheets or a macro imbedded in a Microsoft Word file, email attachments, etc.).

You can select and scan all files or only new ones for each type of compound file. To do so, use the link next to the name of the object. It changes its value when you left-click on it. If the **Productivity** section has been set up only to scan new and modified files, you will not be able to select the type of compound files to be scanned.

- Parse email formats** – scan email files and email databases. If this checkbox is selected, Kaspersky Anti-Virus will parse the mail file and analyze every component of the e-mail (body, attachments) for viruses. If this checkbox is deselected, the mail file will be scanned as a single object.

Please note, when scanning password-protected email databases:

- Kaspersky Anti-Virus detects malicious code in Microsoft Office Outlook 2000 databases but does not disinfect them;
- Kaspersky Anti-Virus does not support scans for malicious code in Microsoft Office Outlook 2003 protected databases.

- Scan password-protected archives** – scans password protected archives. With this feature, a window will request a password before scanned archived objects. If this box is not checked, password-protected archives will be skipped.

11.4.3. Restoring default scan settings

When configuring scan task settings, you can always return to the recommended settings. Kaspersky Lab considers them to be optimal and has combined them in the **Recommended** security level.

To restore the default file scan settings:

1. Select the task name in the **Scan** of the main window. Right-click on the task name to open the context menu, or click the **Actions** button on the right of the list of scan objects, and select **Settings**.
2. Click the **Default** button in the **Security Level** section.

11.4.4. Selecting actions for objects

If a file is found to be infected or suspicious during a scan, the program's next steps depend on the object status and the action selected.

One of the following statuses can be assigned to the object after the scan:

- Malicious program status (for example, *virus*, *Trojan*).
- *Potentially infected*, when the scan cannot determine whether the object is infected. It is likely that the program detected a sequence of code in the file from an unknown virus or modified code from a known virus.

By default, all infected files are disinfected, and if they are potentially infected, they are sent to Quarantine.

To edit an action for an object:

select the task name in the **Scan** section of the main program window and use the [Settings](#) link to open the task settings window. The possible responses are displayed in the appropriate sections(see fig. 45).

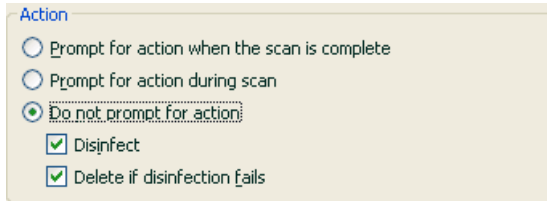


Figure 45. Selecting actions for dangerous objects

| If the action selected was | When it detects an infected or potentially infected object |
|--|---|
| <input type="radio"/> Prompt for action when the scan is complete | The program does not process the objects until the end of the scan. When the scan is complete, the statistics window will pop up with a list of objects detected, and you will be asked if you want to process the objects. |
| <input type="radio"/> Prompt for action during scan | The program will issue a warning message containing information about what malicious code has infected or potentially infected the file, and gives you the choice of one of the following actions. |
| <input checked="" type="radio"/> Do not prompt for action | The program records information about objects detected in the report without processing them or notifying the user. You are advised not to use this feature, since infected and potentially infected objects stay on your computer and it is practically impossible to avoid infection. |
| <input checked="" type="radio"/> Do not prompt for action <input checked="" type="checkbox"/> Disinfect | The program attempts to treat the object detected without asking the user for confirmation. If disinfection fails, the file will be assigned the status of |

| | |
|---|---|
| | <i>potentially infected</i> , and it will be moved to Quarantine (see 14.1 on pg. 153). Information about this is recorded in the report (see 14.3 on pg. 158). Later you can attempt to disinfect this object. |
| <input checked="" type="radio"/> Do not prompt for action <input checked="" type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete if disinfection fails | The program attempts to treat the object detected without asking the user for confirmation. If the object cannot be disinfected, it is deleted. |
| <input checked="" type="radio"/> Do not prompt for action <input type="checkbox"/> Disinfect <input checked="" type="checkbox"/> Delete | The program automatically deletes the object |

When disinfecting or deleting an object, Kaspersky Anti-Virus creates a backup copy of it, and sends it to Backup (see 14.2 on pg. 156) in case the object needs to be restored or an opportunity arises later to treat it.

11.4.5. Advanced virus scan options

In addition to configuring the basic virus scan settings, you can also use additional settings (see fig. 46):

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

For example, you have an archived file that the program scanned and assigned the status of not infected. The next time, the program will skip this archive, unless it has been modified or the scan settings have been changed. If the structure of the archive has changed because a new object has been added to it, if the scan settings have changed, or if the threat signatures have been updated, the program will scan the archive again.

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

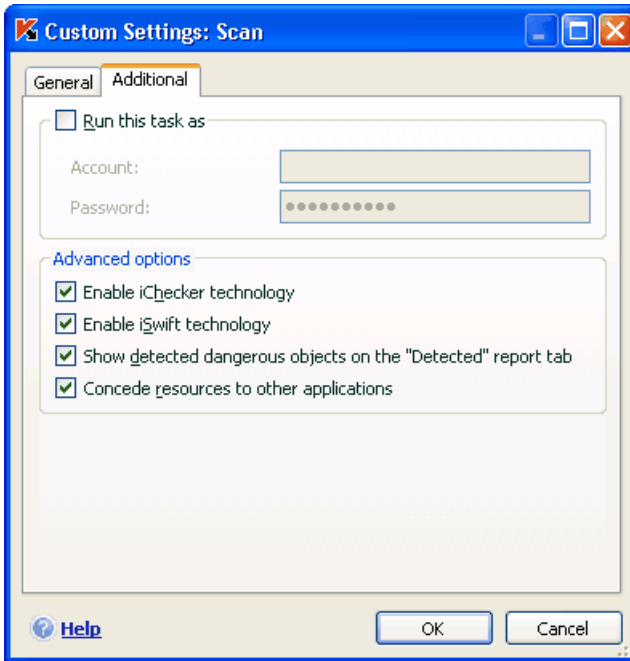


Figure 46. Advanced scan settings

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

iSwift technology is not available on computers running Microsoft Windows 98SE/ME/XP64.

- ✓ **Show detected dangerous objects on the “Detected” report tab** – display a list of threats detected during the scan on the **Detected** tab of the report (see 14.3.2 on pg. 161) window. Disabling this function may be appropriate for special scans, for example of text collections, to increase the scan speed.
- ✓ **Concede resources to other applications** – pause that virus scan task if the processor is busy with other applications.

11.4.6. Setting up global scan settings for all tasks

Each scan task is executed according to its own settings. By default, the tasks created when you install the program on your computer use the settings recommended by Kaspersky Lab.

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

To assign global scan settings for all tasks:

1. Select the **Scan** section in the left-hand part of the main program window and click Settings.
2. In the settings window that opens, configure the scan settings: Select the security level (see 11.4.1 on pg. 125), configure advanced level settings, and select an action (see 11.4.4 on pg. 129) for objects.
3. To apply these new settings to all tasks, click the **Apply** button in the **Other task settings** section. Confirm the global settings that you have selected in the popup dialogue box.


CHAPTER 12. TESTING

KASPERSKY ANTI-VIRUS

FEATURES

After installing and configuring Kaspersky Anti-Virus, we recommend that you verify that settings and program operation are correct using a test virus and variations of it.

12.1. The EICAR test virus and its variations

The test virus was specially developed by  (The European Institute for Computer Antivirus Research) for testing antivirus functionality.

The test virus IS NOT A VIRUS and does not contain program code that could damage your computer. However, most antivirus programs will identify it as a virus.

Never use real viruses to test the functionality of an antivirus!

You can download the test virus from the official **EICAR** website: http://www.eicar.org/anti_virus_test_file.htm.

The file that you downloaded from the **EICAR** website contains the body of a standard test virus. Kaspersky Anti-Virus will detect, label it a **virus**, and take the action set for that object type.

To test the reactions of Kaspersky Anti-Virus when different types of objects are detected, you can modify the contents of the standard test virus by adding one of the prefixes in the table shown here.

| Prefix | Test virus status | Corresponding action when the application processes the object |
|--------------------------------|---|--|
| No prefix, standard test virus | The file contains a test virus. You cannot disinfect the object. | The application will identify the object as malicious and not subject to treatment and will delete it. |
| CORR- | Corrupted. | The application could access the object but could not scan it, since the object is corrupted (for example, the file structure is breached, or it is an invalid file format). |
| SUSP- WARN- | The file contains a test virus (modification). You cannot disinfect the object. | This object is a modification of a known virus or an unknown virus. At the time of detection, the threat signature databases do not contain a description of the procedure for treating this object. The application will place the object in Quarantine to be processed later with updated threat signatures. |
| ERRO- | Processing error. | An error occurred while processing the object: the application cannot access the object being scanned, since the integrity of the object has been breached (for example, no end to a multivolume archive) or there is no connection to it (if the object is being scanned on a network drive). |


| Prefix | Test virus status | Corresponding action when the application processes the object |
|--------|--|---|
| CURE- | <p>The file contains a test virus. It can be cured.</p> <p>The object is subject to disinfection, and the text of the body of the virus will change to CURE.</p> | <p>The object contains a virus that can be cured. The application will scan the object for viruses, after which it will be fully cured.</p> |
| DELE- | <p>The file contains a test virus. You cannot disinfect the object.</p> | <p>This object contains a virus that cannot be disinfected or is a Trojan. The application deletes these objects.</p> |

The first column of the table contains the prefixes that need to be added to the beginning of the string for a standard test virus. The second column describes the status and reaction of Kaspersky Anti-Virus to various types of test virus. The third column contains information on objects with the same status that the application has processed.

Values in the anti-virus scan settings determine the action taken on each of the objects.

12.2. Testing File Anti-Virus

To test the functionality File Anti-Virus;

1. Create a folder on a disk, copy to it the test virus downloaded from the organization's official website (see 12.1 on pg. 134), and the modifications of the test virus that you created.
2. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors. To do so, check  **Log non-critical events** in the report settings window (see 14.3.1 on pg. 161).
3. Run the test virus or a modification of it.

File Anti-Virus will intercept your attempt to access the file, will scan it, and will inform you that it has detected a dangerous object:



Figure 47. Dangerous object detected

When you select different options for dealing with detected objects, you can test File Anti-Virus's reaction to detecting various object types.

You can view details on File Anti-Virus performance in the report on the component.

12.3. Testing Virus scan tasks

To test Virus scan tasks:

1. Create a folder on a disk, copy to it the test virus downloaded from the organization's official website (see 12.1 on pg. 134), and the modifications of the test virus that you created.
2. Create a new virus scan task (see 11.3 on pg. 124) and select the folder containing the set of test viruses as the objects to scan (see 11.2 on pg. 122).
3. Allow all events to be logged so the report file retains data on corrupted objects and objects not scanned because of errors. To do so, check **Log non-critical events** in the report settings window.
4. Run the virus scan task (see 11.1 on pg. 122).

When you run a scan, as suspicious or infected objects are detected, notifications will be displayed on screen will information about the objects, prompting the user for the next action to take:

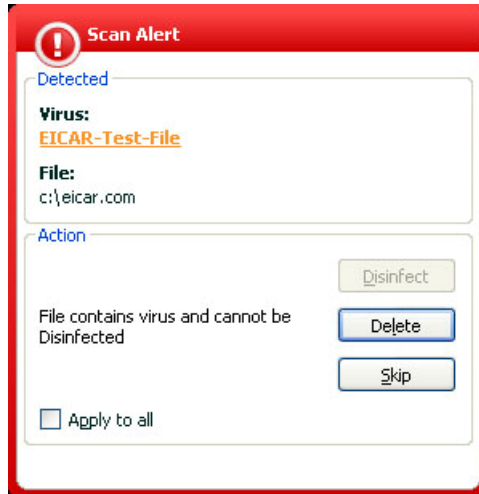


Figure 48. Dangerous object detected

This way, by selecting different options for actions, you can test Kaspersky Anti-Virus reactions to detecting various object types.

You can view details on virus scan task performance in the report on the component.

CHAPTER 13. PROGRAM UPDATES

Keeping your anti-virus software up-to-date is an investment in your computer's security. Because new viruses, Trojans, and malicious software emerge daily, it is important to regularly update the application to keep your information constantly protected. This task is managed by the *Updater* component.

Updating the application involves the following components being downloaded and installed on your computer:

- **Threat Signatures**

The application uses threat signatures to protect information on your computer. The software components that provide protection use the database of threat signatures to search for and disinfect harmful objects on your computer. The signatures are added to every hour, with records of new threats and methods to combat them. Therefore, it is recommended that they are updated on a regular basis.

In addition to the threat signatures, network drivers that enable protection components to intercept network traffic are updated.

Previous versions of Kaspersky Lab applications have supported *standard* and *extended* database sets. Each database dealt with protecting your computer against different types of dangerous objects. In Kaspersky Anti-Virus you don't need to worry about selecting the appropriate threat signature set. Now our products use an threat signatures that protect you from both malicious and potentially dangerous objects, and from hacker attacks.

- **Application modules**

In addition to the signatures, you can upgrade the internal modules of Kaspersky Anti-Virus. New application updates appear regularly.

The main update source for Kaspersky Anti-Virus is Kaspersky Lab's update servers. These are a few of the addresses:

<http://downloads1.kaspersky-labs.com/updates/>

<http://downloads2.kaspersky-labs.com/updates/>

<ftp://downloads1.kaspersky-labs.com/updates/>

To download available updates from the update servers, your computer must be connected to the Internet.

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

Updates can be downloaded in one of the following modes:

- *Auto.* Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scans can be set to be more frequent during virus outbreaks and less so when they are over. When the program detects fresh updates, it downloads them and installs them on the computer. This is the default setting.
- *By schedule.* Updating is scheduled to start at a specified time.
- *Manual.* With this option, you launch the Updater manually.

During updating, the application compares the threat signatures and application modules on your computer with the versions available on the update server. If your computer has the latest version of the signatures and application modules, you will see a notification window confirming that your computer is up-to-date. If the signatures and modules on your computer differ from those on the update server, only the missing part of the updates will be downloaded. The Updater does not download threat signatures and modules that you already have, which significantly increases download speed and saves Internet traffic.

Before updating threat signatures, Kaspersky Anti-Virus creates backup copies of them, that can be used if a rollback (see 13.2 on pg. 141) is required. If, for example, the update process corrupts the threat signatures and leaves them unusable, you can easily roll back to the previous version and try to update the signatures later.

You can distribute the updates retrieved to a local source while updating the application (see 13.4.4 on pg. 149). This feature allows you to update databases and modules used by 6.0 duplications on networked computers to conserve bandwidth.

13.1. Starting the Updater

You can begin the update process at any time. It will run from the update source that you have selected (see 13.4.1 on pg. 143).


You can start the Updater from:

- the context menu (see 4.2 on pg. 39).
- from the program's main window (see 4.3 on pg. 40)

To start the Updater from the shortcut menu:

1. Right click the application icon in the system tray to open the shortcut menu.
2. Select **Update**.

To start the Updater from the main program window:

1. Select **Update** in the **Service** section.
2. Click the **Update now!** Button in the right panel of the main window or use the  button on the status bar.

The update progress will be displayed in a special window, which can be hidden by clicking **Close**. The update will continue with the window hidden.

Note that updates are distributed to the local source during the update process, provided that this service is enabled (see 13.4.4 on pg. 149).

13.2. Rolling back to the previous update

Every time you start the Updater, Kaspersky Anti-Virus creates a backup copy of the current threat signatures before it starts downloading updates. This way you can return to using the previous version of signatures if an update fails.

The rollback option can be helpful if, for example, the update process fails because of a connection error. You can roll back to the previous threat signatures and try to update it again later.

To rollback to the previous version of threat signatures:

1. Select the **Update** component in the **Service** section of the main program window.
2. Click the **Rollback** button in the right panel of the main program window.

13.3. Creating update tasks

Kaspersky Anti-Virus has a built-in update task for updating program modules and threat signatures. You can also create your own update tasks with various settings and start schedules.

For example, you installed Kaspersky Anti-Virus on a laptop that you use at home and at your office. At home, you update the program from the Kaspersky Lab update servers, and at the office, from a local folder that stores the updates you need. Use two different tasks to avoid having to change update settings every time you change locations.

To create an advanced update task:

1. Select **Update** from the **Service** section of the main program window, open the context menu by right-clicking, and select **Save as**.
2. Enter the name for the task in the window that opens and click **OK**. A task with that name will then appear in the **Service** section of the main program window.

Warning!

There is a limit to the number of update tasks that the user can create. Maximum number: two tasks.

The new task inherits all the properties of the task it is based on, except for the schedule settings. The default automatic scan setting for the new task is disabled.

After creating a task, configure additional settings: specify the update source (see 13.4.1 on pg. 143), network settings (see 13.4.3 on pg. 147), and if necessary enable tasks with privileges (see 6.4 on pg. 131) and configure the schedule (see 6.5 on pg. 69).

To rename a task:

Select the task from the **Service** section of the main program window, open the context menu by right-clicking, and select **Rename**.

Enter the new name for the task in the window that opens and click **OK**. The task name will then be changed in the **Service** section.

To delete a task:

Select the task from the **Service** section of the main program window, open the context menu by right-clicking, and select **Delete**.

Confirm that you want to delete the task in the confirmation window. The task will then be deleted from the list of tasks in the **Service** section.

Warning!

Rename and delete are only available for customized tasks.

13.4. Configuring update settings

The Updater settings specify the following parameters:

- The source from which the updates are downloaded and installed (see 13.4.1 on pg. 143)
- The run mode for the updating procedure (see 13.4.2 on pg. 145)
- Which objects are updated
- What actions are to be performed after updating is complete (see 13.4.4 on pg. 149)

The following sections examine these aspects in detail.

13.4.1. Selecting an update source

The *update source* is where you download updates for the threat signatures and Kaspersky Anti-Virus internal modules.

The chief source of updates is *Kaspersky Labs update servers*. These are special web sites containing available updates for the threat signatures and internal modules for all Kaspersky Lab products.

If you cannot access Kaspersky Lab's update servers (for example, you have no Internet connection), you can call the Kaspersky Lab main office at +7 (495) 797-87-00 to request contact information for Kaspersky Lab partners, who can provide zipped updates on floppy disks or CDs.

Warning!

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

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

Select the update source on the **Update Source** tab (see fig. 49).

The default option download updates from Kaspersky Lab update servers.. The list of addresses which this item represents cannot be edited. When updating, Kaspersky Anti-Virus calls this list, selects the address of the first server, and tries to download files from this server. If updates cannot be downloaded from the first server, the application tries to connect to each of the servers in turn until it is successful. The address of the server from which updates were successfully downloaded is automatically placed at the top of the list, so that next time the application will try to connect to this server first.

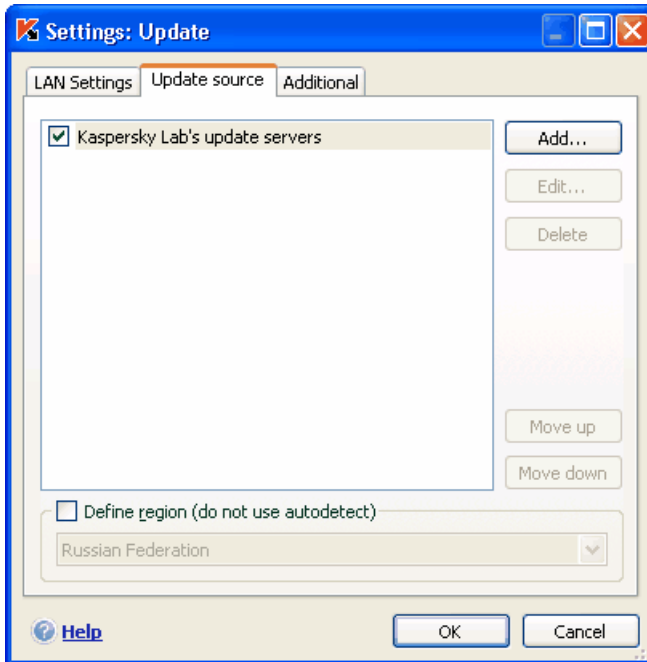


Figure 49. Selecting an update source

To download updates from another FTP or HTTP site:

1. Click **Add**.
2. In the **Select update source** dialog box, select the target FTP or HTTP site or specify the IP address, character name, or URL address of this site in the **Source** field.

Warning!

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

To update from a local folder:

1. Click **Add**.
2. In the **Select update source** dialog box, select a folder or specify the full path to this folder in the **Source** field.

Kaspersky Anti-Virus adds new update sources at the top of the list, and automatically enables the source, by checking the box beside the source name.

If several resources are selected as update sources, the application tries to connect to them one after another, starting from the top of the list, and retrieves the updates from the first available source. You can change the order of sources in the list using the **Move up** and **Move down** buttons.

To edit the list, use the **Add**, **Edit** and **Remove** buttons. The only source you cannot edit or delete is the one labeled Kaspersky Lab's update servers.

If you use Kaspersky Lab's update servers as the update source, you can select the optimal server location for downloading updates. Kaspersky Lab has servers in several countries. Choosing the Kaspersky Lab update server closest to you will save you time and download updates faster.

To choose the closest server, check **Define region (do not use autodetect)** and select the country closest to your current location from the dropdown list. If you check this box, updates will run taking the region selected in the list into account. This checkbox is deselected by default and information about the current region from the operating system registry is used.

13.4.2. Selecting an update method and what to update

When configuring updating settings, it is important to define what will be updated and what update method will be used.

Update objects (see fig. 50) are the components that will be updated:

- threat signatures
- Application modules;
- network drivers that enable protection components to intercept network traffic.

The threat signatures are always updated, and the application modules and network drivers are only updated if the settings are configured for it.

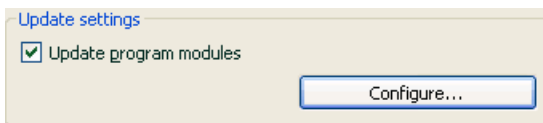


Figure 50. Selecting update objects

If you want to download and install updates for program modules:

Check **Update application modules** in the **Settings** dialog box of the **Update** service.

If there are currently program module updates on the update source, the program will download the updates it needs and apply them after the computer restarts. The module updates will not be installed until the computer is restarted.

If the next program update occurs before the computer is restarted and before the previous program module updates were installed, only the threat signatures will be updated.

If you want to download and install the network drivers database:

Check **Update network drivers** in the settings window of the **Update** component.

Run Mode (see fig. 51) defines how the Updater is started. You can select one of these methods:

Automatically. Kaspersky Anti-Virus checks the update source for update packages at specified intervals (see 0 on pg. 143). When the program detects fresh updates, it downloads them and installs them on the computer. This mode is used by default.

If you have a dialup Internet connection and a network resource is specified as an update source, Kaspersky Anti-Virus tries to start the Updater each time the computer connects to that resource, or after a certain amount of time has elapsed as specified in the previous update packet.

If a local folder is selected as an update source, the application tries to download the updates from the local folder as often as specified in the update package that was downloaded during the previous update. This option allows Kaspersky Lab to regulate how often the program is updated in case of virus outbreaks and other potentially dangerous situations. Your application will receive the latest updates for the threat signatures, network attacks, and software modules in a timely manner, thus preventing malicious software to penetrate your computer.

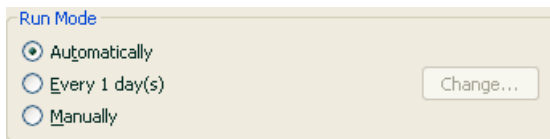



Figure 51. Selecting an update run mode

Every 1 day(s) The Updater is scheduled to start at a specified time. The default schedule runs the Updater daily. To edit the default schedule, click the **Change...** button in the **Run Mode** box and make the necessary changes in the window that opens (for more details, see 6.5 on pg. 69).

 **Manually.** With this option, you start the Updater manually. Kaspersky Anti-Virus notifies you when it needs to be updated:

- A popup message, informing you that updating is required, appears above the application icon in the system tray (in notices are enabled; see 14.11.1 on pg. 180)
- The second indicator in the main program window informs you that your computer is out-of-date (see 5.1.1 on pg. 46)
- A recommendation, that the application needs updating, appears in the message section in the main program window (see 4.3 on pg. 40)

13.4.3. Configuring connection settings

If you set up the program to retrieve updates from Kaspersky Lab's update servers, or from other FTP or HTTP sites, you are advised to first check your connection settings.

By default, to establish an Internet connection, the application uses the settings of Microsoft Internet Explorer. To change the connection settings, you should know whether a proxy server is being used and whether you are behind a firewall. If you do not know this information, contact your system administrator or Internet provider.

All settings are grouped on a special tab – **LAN Settings** (see fig. 52).

Check **Use passive FTP mode if possible** if you download the updates from an FTP server in passive mode (for example, through a firewall). If you are working in active FTP mode, clear this checkbox.

In the **Connection timeout ... (sec)** field, assign the time allotted for connection with the update server. If the connection fails, once this time has elapsed the program will attempt to connect to the next update server. This continues until a connection is successfully made or until all the available update servers are attempted.

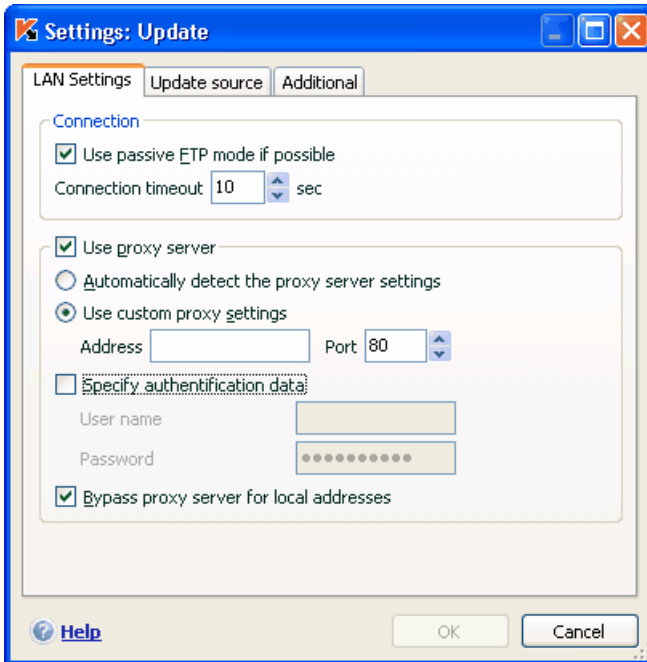


Figure 52. Configuring network update settings

Check **Use proxy server** if you are using a proxy server to access the Internet and, if necessary, select the following settings:

- Select the proxy server settings that will be used during updating:
 - **Automatically detect proxy server settings.** If you select this option, the proxy settings are detected automatically using WPAD (Web Proxy Auto-Discovery Protocol). If this protocol cannot detect the address, Kaspersky Anti-Virus will use the proxy server settings specified in Microsoft Internet Explorer.
 - **Use custom proxy settings** – Use a proxy that is different from that specified in the browser connection settings. In the **Address** field, enter either the IP address or the symbolic name of the proxy server, and specify the number of the proxy port used to update the application in the **Port** field.
- Specify whether authentication is required on the proxy server. *Authentication* is the process of verifying user registration data for access control purposes.

If authentication is required to connect to the proxy server, check Proxy requires authorization and specify the username and password in the fields below. In this event, first NTLM authentication and then BASIC authentication will be attempted. If this checkbox is not selected or if the data is not entered, NTLM authentication will be attempted using the user account used to start the update (see 0 on pg. 131).

If the proxy server requires authentication and you did not enter the username and password or the data specified were not accepted by the proxy server for some reason, a window will pop up when updates start, asking for a username and password for authentication. If authentication is successful, the username and password will be used when the program is next updated. Otherwise, the authentication settings will be requested again.

To avoid using a proxy when the update source is a local folder, select the **Bypass proxy server for local addresses.**

This feature is unavailable under Microsoft Windows 9X/NT 4.0. However, the proxy server is by default not used for local addresses.

13.4.4. Update distribution

If your home computers are connected through a home network, you do not need to download and installed updates on each of them separately, since this would consume more network bandwidth. You can use the update distribution feature, which helps reduce traffic by retrieving updates in the following manner:

1. One of the computers on the network retrieves an application and threat signature update package from the Kaspersky Lab web servers or from another web resources hosting a current set of updates. The updates retrieved are placed in a public access folder.
2. Other computers on the network access the public access folder to retrieve application updates.

To enable update distribution, select the **Update distribution folder** checkbox on the **Additional** tab (see Figure 53), and in the field below, specify the shared folder where updates retrieved will be placed. You can enter the path manually or selected in the window that opens when you click **Browse**. If the checkbox is selected, updates will automatically be copied to this folder when they are retrieved.

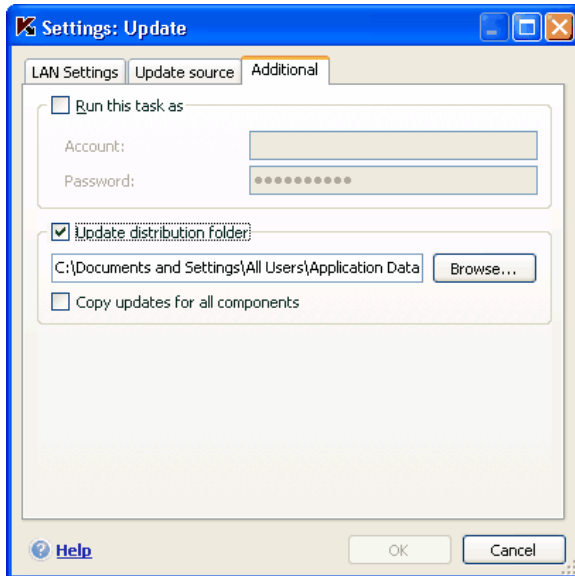


Figure 53. Update distribution tool settings

You can also specify the method for update distribution:

- *complete*, which copies threat signatures and component updates for all Kaspersky Lab 6.0 applications. To select complete updates, select the **Copy updates for all components** checkbox.
- *custom*, which only copies threat signatures and updates for the Kaspersky Anti-Virus 6.0 components that are installed. If you want to select this update method, you must deselect the **Copy updates for all components** checkbox.

If you want other computers on the network to update from the folder that contains updates copied from the Internet, you must take the following steps:

1. Grant public access to this folder.
2. Specify the shared folder as the update source on the network computers in the Updater settings.

13.4.5. Actions after updating the program

Every threat signature update contains new records that protect your computer from the latest threats.

Kaspersky Lab recommends that you scan *quarantined objects* and *startup objects* each time after the database is updated.

Why these objects should be scanned?

The quarantine area contains objects that have been flagged by the program as suspicious or possibly infected (see 14.1 on pg. 153). Using the latest version of the threat signatures, Kaspersky Anti-Virus may be able to identify the threat and eliminate it.

By default, the application scans quarantined objects after each threat signature update. You are also advised to periodically view the quarantined objects because their statuses can change after several scans. Some objects can then be restored to their previous locations, and you will be able to continue working with them.

To disable scans of quarantined objects, uncheck **Rescan Quarantine** in the **Actions after Update** section.

Startup objects are critical for the safety of your computer. If one of them is infected with a malicious application, this could cause an operating system startup failure. Kaspersky Anti-Virus has a built-in scan task for startup objects (see Chapter 11 on pg. 121). You are advised to set up a schedule for this task so that it is launched automatically after each threat signature update (see 6.5 on pg. 69).

CHAPTER 14. ADVANCED OPTIONS

Kaspersky Anti-Virus has other features that expand its functionality.

The program places some objects in special storage areas, in order to ensure maximum protection of data with minimum losses.

- Backup contains copies of objects that Kaspersky Anti-Virus has changed or deleted (see 14.2 on pg. 156). If any object contained information that was important to you and could not be fully recovered during anti-virus processing, you can always restore the object from its backup copy.
- Quarantine contains potentially infected objects that could not be processed using the current threat signatures (see 14.1 on pg. 153).

It is recommended that you periodically examine the list of stored objects. Some of them may already be outdated, and some may have been restored.

The advanced options include a number of diverse useful features. For example:

- Technical Support provides comprehensive assistance with Kaspersky Anti-Virus (see 14.5 on pg. 168). Kaspersky provides you with several channels for support, including on-line support and a questions and comments forum for program users.
- The Notifications feature sets up user notifications about key events for Kaspersky Anti-Virus (see 14.11.1 on pg. 180). These could be either events of an informative nature, or critical errors that must be eliminated immediately.
- Self-Defense protects the program's own files from being modified or damaged by hackers, blocks remote administration from using the program's features, and restricts other users on your computer from performing certain actions in Kaspersky Anti-Virus (see 14.11.1.3 on pg. 184). For example, changing the level of protection can significantly influence information security on your computer.
- License Key Manager can obtain detailed information on the license used, activate your copy of the program, and manage license key files (see 14.5 on pg. 168).

The program also provides a Help section (see 14.4 on pg. 167) and detailed reports (see 14.3 on pg. 158) on the operation of all protection components and virus scan tasks.

Monitored ports can regulate which Kaspersky Anti-Virus modules control data transferred on select ports (see 14.7 on pg. 171).

The Rescue Disk can help restore your computer's functionality after an infection (see 14.10 on pg. 176). This is particularly helpful when you cannot boot your computer's operating system after malicious code has damaged system files.

You can also change the appearance of Kaspersky Anti-Virus and can customize the program interface (see 14.8 on pg. 173).

The following sections discuss these features in more detail.

14.1. Quarantine for potentially infected objects

Quarantine is a special storage area that holds potentially infected objects.

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

Why *potentially infected*? This are several reasons why it is not always possible to determine whether an object is infected:

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

Threat signatures contain threats that have already been studied by Kaspersky Lab. If a malicious program is modified by a hacker but these changes have not yet been entered into the signatures, Kaspersky Anti-Virus classifies the object infected with this changed malicious program as being potentially infected, and indicates what threat this infection resembles.

- *The code of the object detected is reminiscent in structure of a malicious program, although nothing similar is recorded in the threat signatures.*

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

The *heuristic code* analyzer detects potential viruses, identifying up to 92% of new viruses. This mechanism is fairly effective and very rarely produces false positives.

A potentially infected object can be detected and placed in quarantine by [File Anti-Virus](#), [Mail Anti-Virus](#), [Proactive Defense](#) or in the course of a [virus scan](#).

You can place an object in quarantine by clicking **Quarantine** in the notification that pops up when a potentially infected object is detected.

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

14.1.1. Actions with quarantined objects

The total number of objects in Quarantine is displayed by selecting the **Data files** item in the **Service** area of the application's main window. In the right-hand part of the screen the *Quarantine* section displays:

- the number of potentially infected objects detected during Kaspersky Anti-Virus operation;
- the current size of Quarantine.

Here you can delete all objects in the quarantine with the **Clean** button. Note that in doing so the Backup files and report files will also be deleted.

To access objects in Quarantine:

Left-click in any part of the *Quarantine* box to open the Protection window which summarises protection given by the application.

You can take the following actions on the Quarantine tab (see fig. 54):

- Move a file to Quarantine that you suspect is infected but the program did not detect. To do so, click **Add** and select the file in the standard selection window. It will be added to the list with the status *added by user*.
- Scan and disinfect all potentially infected objects in Quarantine using the current threat signatures by clicking, click **Scan all**.

After scanning and disinfecting any quarantined object, its status may change to *infected*, *potentially infected*, *false positive*, *OK*, etc.

The *infected* status means that the object has been identified as infected but it could not be treated. You are advised to delete such objects.

All objects marked *false positive* can be restored, since their former status as *potentially infected* was not confirmed by the program once scanned again.

- Restore the files to a folder selected by the user or their original folder prior to Quarantine (default). To restore an object, select it from the list and click **Restore**. When restoring objects from archives, email databases, and email format files placed in Quarantine, you must also select the directory to restore them to.

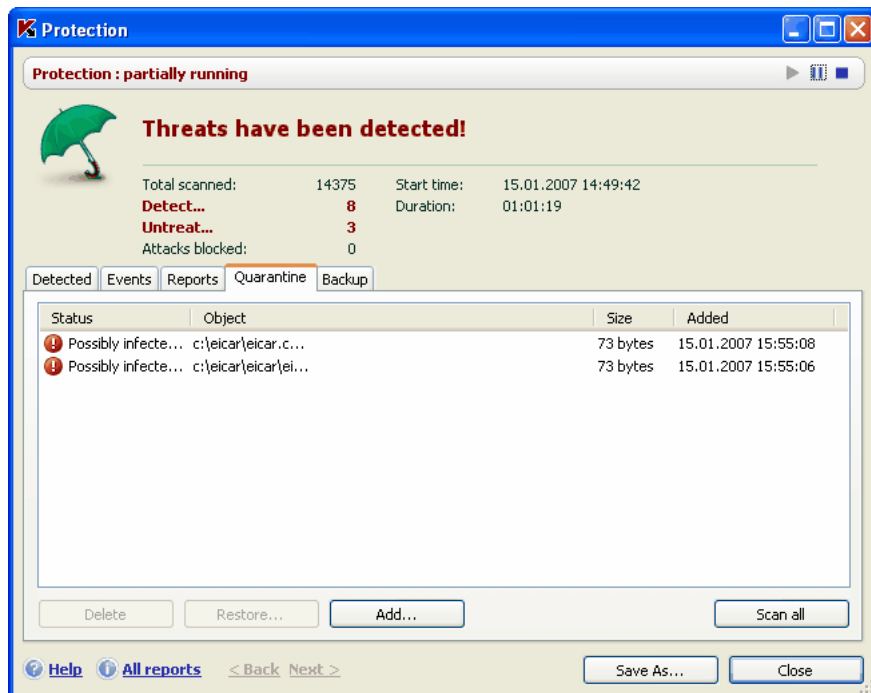


Figure 54. List of quarantined objects

Tip:

We recommend that you only restore objects with the status *false positive*, *OK*, and *disinfected*, since restoring other objects could lead to infecting your computer.

- Delete any quarantined object or group of selected objects. Only delete objects that cannot be disinfected. To delete the objects, select them in the list and click **Delete**.

14.1.2. Setting up Quarantine

You can configure the settings for the layout and operation of Quarantine, specifically:

- Set up automatic scans for objects in Quarantine after each threat signature update (for more details, see 13.4.4 on pg. 149).

Warning!

The program will not be able to scan quarantined objects immediately after updating the threat signatures if you are accessing the Quarantine area.

- Set the maximum Quarantine storage time.

The default storage time 30 days, at the end of which objects are deleted. You can change the Quarantine storage time or disable this restriction altogether.

To do so:

1. Open the Kaspersky Anti-Virus settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. In the **Quarantine & Backup** section (see fig. 55), enter the length of time after which objects in Quarantine will be automatically deleted. Alternately, uncheck the checkbox to disable automatic deletion.



Figure 55. Configuring the Quarantine storage period

14.2. Backup copies of dangerous objects

Sometimes when objects are disinfected their integrity is lost. If a disinfected file contains important information which is partially or fully corrupted, you can attempt to restore the original object from a backup copy.

A **backup copy** is a copy of the original dangerous object that is created before the object is disinfected or deleted. It is saved in Backup.

Backup is a special storage area that contains backup copies of dangerous objects. Files in backup are saved in a special format and are not dangerous.

14.2.1. Actions with backup copies

The total number of backup copies of objects in Backup is displayed in the **Data files** in the **Service** section of the application's main window. In the right-hand part of the screen the *Backup* section displays:

- the number of backup copies of objects created by Kaspersky Anti-Virus
- the current size of Backup.

Here you can delete all the copies in Backup with the **Clean up** button. Note that in doing so the Quarantine objects and report files will also be deleted.

To access dangerous object copies:

Left-click anywhere in the *Backup* box to open the **Protection** window, which summarises protection given by the application.

A list of backup copies is displayed in the Backup tab (see fig. 56). The following information is displayed for each copy: the full path and filename of the object, the status of the object assigned by the scan, and its size.

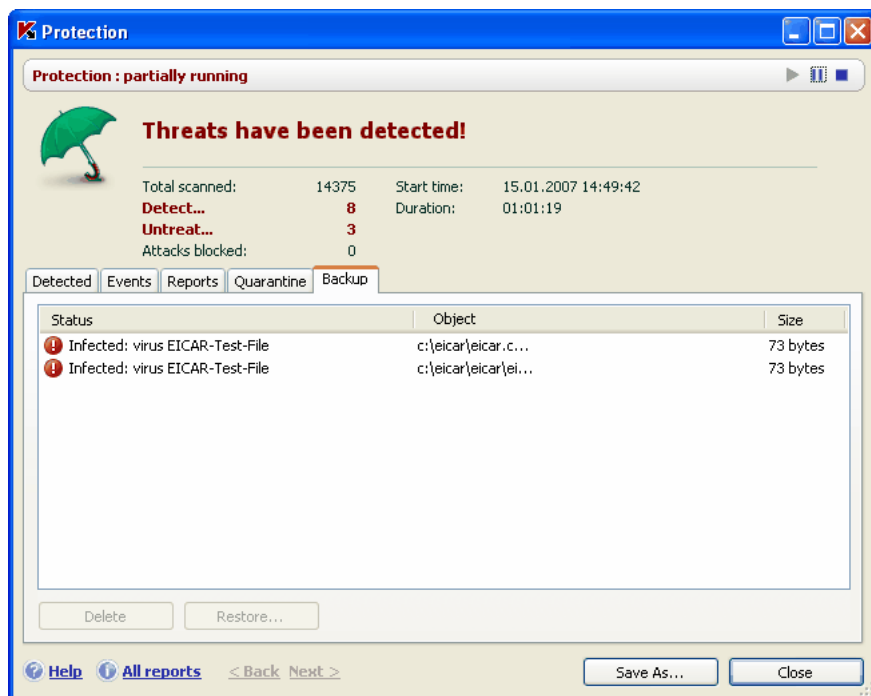


Figure 56. Backup copies of deleted or disinfected objects

You can restore selected copies using the **Restore** button. The object is restored from Backup with the same name that it had prior to disinfection.

If there is an object in the original location with that name (this is possible if a copy was made of the object being restored prior to disinfection), a warning will be given. You can change the location of the restored object or rename it.

You are advised to scan backup objects for viruses immediately after restoring them. It is possible that with updated signatures you will be able to disinfect it without losing file integrity.

You are advised not to restore backup copies of objects unless absolutely necessary. This could lead to an infection on your computer.

You are advised to periodically examine the Backup area, and empty it using the **Delete** button. You can also set up the program so that it automatically deletes the oldest copies from Backup (see 14.2.2 on pg. 158).

14.2.2. Configuring Backup settings

You can define the maximum time that backup copies remain in the Backup area.

The default Backup storage time is 30 days, at the end of which backup copies are deleted. You can change the storage time or remove this restriction altogether. To do so:

1. Open the Kaspersky Anti-Virus settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. Set the duration for storing backup copies in the repository in the **Quarantine & Backup** section (see fig. 55) on the right-hand part of the screen. Alternately, uncheck the checkbox to disable automatic deletion.

14.3. Reports

Kaspersky Anti-Virus component actions, virus task scans and updates are all recorded in reports.

The total number of reports created by the program and their total size is displayed by clicking on **Data files** in the **Service** section of the main program window. The information is displayed in the *Reports* box.

To view reports:

Left-click anywhere in the *Reports* box to open the Protection window, which summarises protection given by the application. The window will open to the **Reports** tab (see fig. 57).

The Reports tab lists the latest reports on all components and virus scan tasks run during the current session of Kaspersky Anti-Virus. The status is listed beside each component or task, for example, *stopped* or *complete*. If you want to view the full history of report creation for the current session of the program, check **Show report history**.

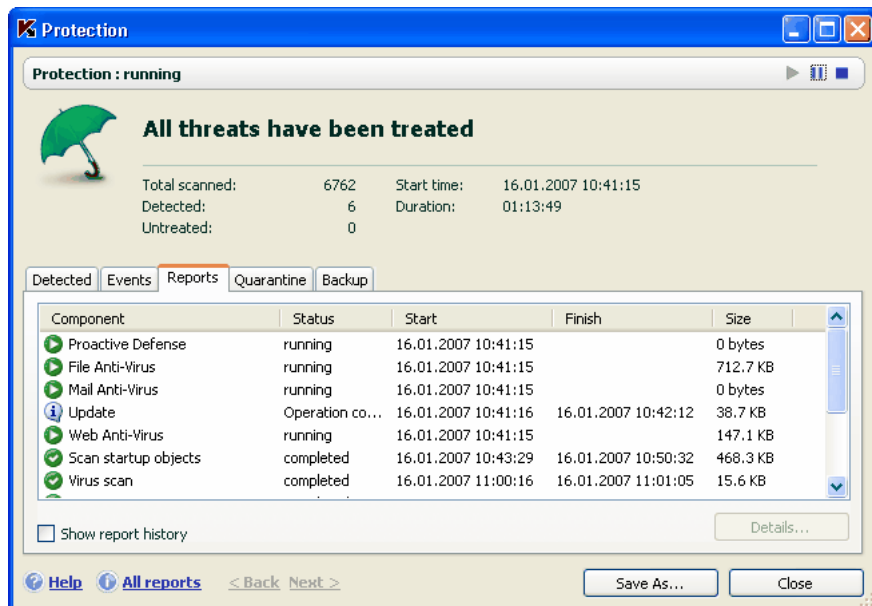


Figure 57. Reports on component operation

To review all the events reported for a component or task:

Select the name of the component or task on the **Reports** tab and click the **Details** button.

A window will then open that contains detailed information on the performance of the selected component or task. The resulting performance statistics are displayed in the upper part of the window, and detailed information is provided on the tabs. Depending on the component or task, the tabs can vary:

- The **Detected** tab contains a list of dangerous objects detected by a component or a virus scan task.
- The **Events** tab displays component or task events.
- The **Statistics** tab contains detailed statistics for all scanned objects.

- The **Settings** tab displays settings used by protection components, virus scans, or threat signature updates.
- The **Macros** and **Registry** tabs are only in the Proactive Defense report and contain information about all macros which attempted to run on your computer, and on all attempts to modify the operating system registry.

You can export the entire report as a text file. This feature is useful when an error has occurred which you cannot eliminate on your own, and you need assistance from Technical Support. If this happens, the report must be sent as a .txt file to Technical Support to enable our specialists can study the problem in detail and solve it as soon as possible.

To export a report as a text file:

Click **Save as** and specify where you want to save the report file.

After you are done working with the report, click **Close**.

There is an Actions button on all the tabs (except **Settings** and **Statistics**) which you can use to define responses to objects on the list. When you click it, a context-sensitive menu opens with a selection of these menu items (the menu differs depending on the component – all the possible options are listed below):

Disinfect – attempts to disinfect a dangerous object. If the object is not successfully disinfected, you can leave it on this list to scan later with updated threat signatures or delete it. You can apply this action to a single object on the list or to several selected objects.

Discard – delete record on detection of the object from the report.

Add to trusted zone – exclude the object from protection. A window will open with an exclusion rule for the object.

Go to File – open the folder where the object is located in Windows Explorer.

Neutralize All – neutralize all objects on the list. Kaspersky Anti-Virus will attempt to process the objects using threat signatures.

Discard All – clear the report on detected objects. When you use this function, all detected dangerous objects remain on your computer.

View on www.viruslist.com – go to a description of the object in the Virus Encyclopedia on the Kaspersky Lab website.

Search www.google.com – find information on the object using this search engine.

Search – enter search terms for objects on the list by name or status.

In addition, you can sort the information displayed in the window in ascending and descending order for each of the columns, by clicking on the column head.

14.3.1. Configuring report settings

To configure settings for creating and saving reports:

1. Open the Kaspersky Anti-Virus settings window by clicking Settings in the main program window.
2. Select **Data files** from the settings tree.
3. Edit the settings in the **Reports** box (see fig. 58) as follows:
 - Allow or disable logging informative events. These events are generally not important for security. To log events, check **Log non-critical events**;
 - Choose only to report events that have occurred since the last time the task was run. This saves disk space by reducing the report size. If **Keep only recent events** is checked, the report will begin from scratch every time you restart the task. However, only non-critical information will be overwritten.
 - Set the storage time for reports. By default, the report storage time is 30 days, at the end of which the reports are deleted. You can change the maximum storage time or remove this restriction altogether.

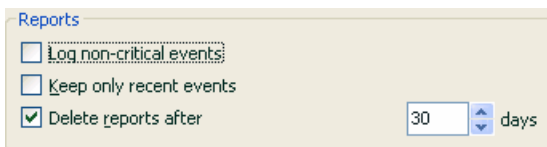


Figure 58. Configuring report settings

14.3.2. The *Detected* tab

This tab (see fig. 59) contains a list of dangerous objects detected by Kaspersky Anti-Virus. The full filename and path is shown for each object, with the status assigned to it by the program when it was scanned or processed.

If you want the list to contain both dangerous objects and successfully neutralized objects, check **Show neutralized objects**.

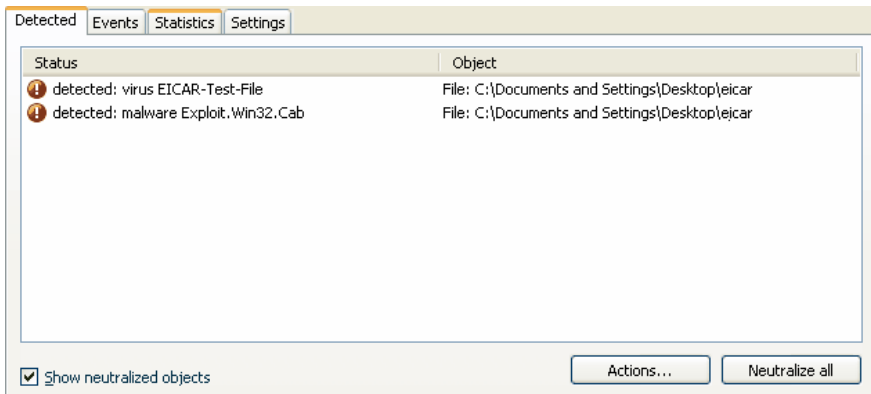


Figure 59. List of detected dangerous objects

Dangerous objects detected by Kaspersky Anti-Virus are processed using the **Neutralize** button (for one object or a group of selected objects) or **Neutralize all** (to process all the objects on the list). When each object is processed, a notification will be displayed on the screen, where you must decide what actions will be taken next.

If you check **Apply to all** in the notification window, the selected action will be applied to all objects with the same status selected from the list before beginning processing.

14.3.3. The *Events* tab

This tab (see fig. 60) provides you with a complete list of all the important events in component operation, virus scans, and threat signature updates that were not overridden by an activity control rule (see 10.1.1 on pg. 106).

These events can be:

Critical events are events of a critical importance that point to problems in program operation or vulnerabilities on your computer. For example, *virus detected*, *error in operation*.

Important events are events that must be investigated, since they reflect important situations in the operation of the program. For example, *stopped*.

Informative messages are reference-type messages which generally do not contain important information. For example, *OK*, *not processed*. These events are only reflected in the event log if **Show all events** is checked.

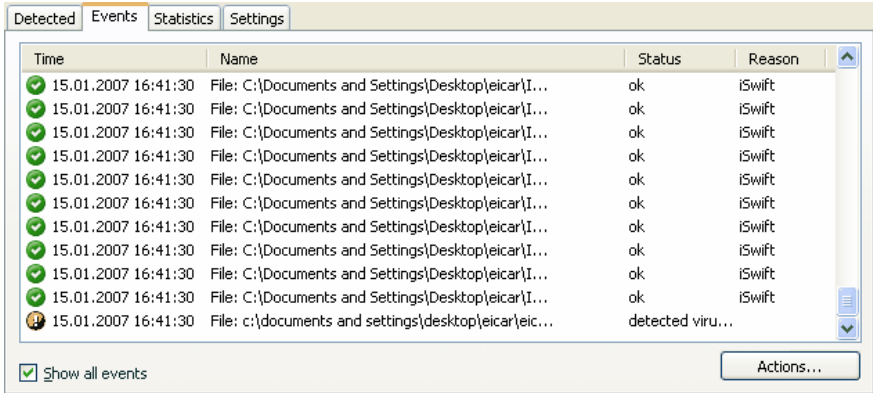


Figure 60. Events that take place in component operation

The format for displaying events in the event log may vary with the component or task. The following information is given for update tasks:

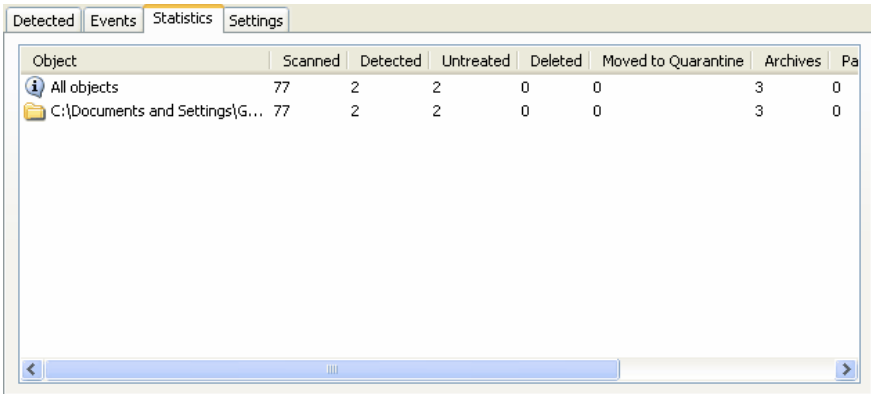
- Event name
- Name of the object involved in the event
- Time when the event occurred
- Size of the file loaded

For virus scan tasks, the event log contains the name of the object scanned and the status assigned to it by the scan/processing.

14.3.4. The Statistics tab

This tab (see fig. 61) provides you with detailed statistics on components and virus scan tasks. Here you can learn:

- How many objects were scanned for dangerous traits in this session of a component, or after a task is completed. The number of scanned archives, compressed files, and password protected and corrupted objects is displayed.
- How many dangerous objects were detected, not disinfected, deleted, or placed in Quarantine.



| Object | Scanned | Detected | Untreated | Deleted | Moved to Quarantine | Archives | Pa |
|--------------------------------|---------|----------|-----------|---------|---------------------|----------|----|
| All objects | 77 | 2 | 2 | 0 | 0 | 3 | 0 |
| C:\Documents and Settings\G... | 77 | 2 | 2 | 0 | 0 | 3 | 0 |

Figure 61. Component statistics

14.3.5. The Settings tab

The **Settings** tab (see fig. 62) displays a complete overview of the settings for components, virus scans and program updates. You can find out the current security level for a component or virus scan, what actions are being taken with dangerous objects, or what settings are being used for program updates. Use the [Change settings](#) link to configure the component.

You can configure advanced settings for virus scans:

- Establish the priority of scan tasks used if the processor is heavily loaded. The default setting for **Consede resources to other applications** is unchecked. With this feature, the program tracks the load on the processor and disk subsystems for the activity of other applications. If the load on the processor increases significantly and prevents the user's applications from operating normally, the program reduces scanning activity. This increases scan time and frees up resources for the user's applications.

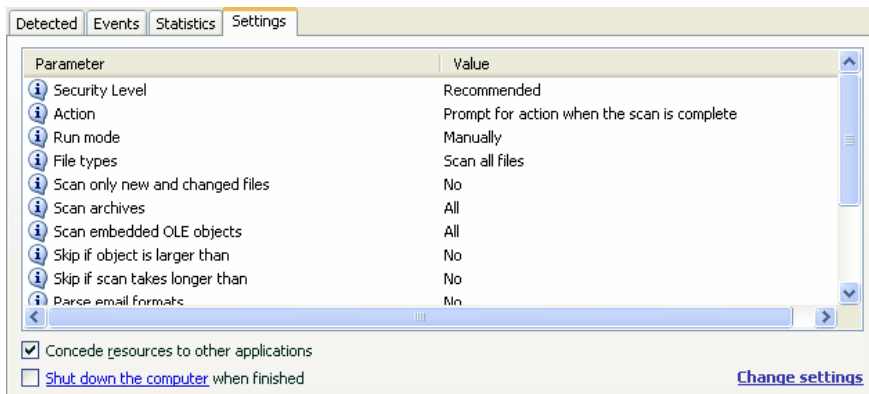


Figure 62. Component settings

- Set the computer's mode of operation for after a virus scan is complete. You can configure the computer to shut down, restart, or go into standby or sleep mode. To select an option, left-click on the hyperlink until it displays the option you need.

You may need this feature if, for example, you start a virus scan at the end of the work day and do not want to wait for it to finish.

However, to use this feature, you must take the following additional steps: before launching the scan, you must disable password requests for objects being scanned, if enabled, and enable automatic processing of dangerous objects, to disable the program's interactive features.

14.3.6. The *Macros* tab

All the macros that attempted to run during the current Kaspersky Anti-Virus session are listed on the **Macros** tab (see Figure 63). Here you will find the full name of each macro, the time it was executed, and its status after macro processing.

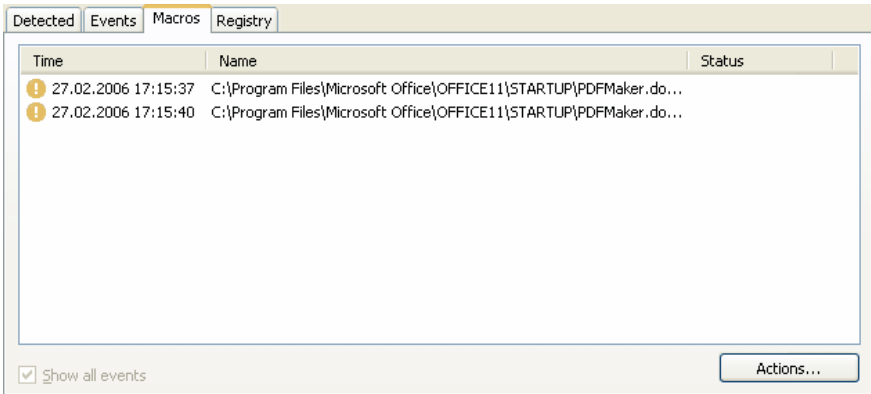


Figure 63. Detected dangerous macros

You can choose view mode for this tab. If you don't want to view informational events uncheck **Show all events**.

14.3.7. The *Registry* tab

The program records operations with registry keys that have been attempted since the program was started on the **Registry** tab (see fig. 64), unless forbidden by a rule (see 10.1.4.2 on pg. 119).

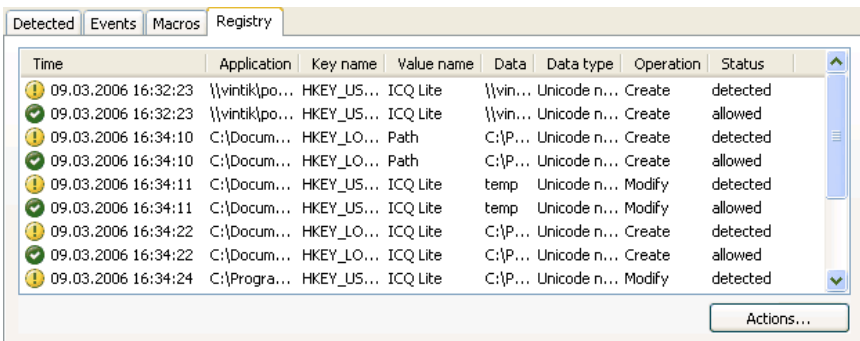


Figure 64. . Read and modify system registry events

The tab lists the full name of the key, its value, the data type, and information about the operation that has taken place: what action was attempted, at what time, and whether it was allowed.

14.4. General information about the program

You can view general information on the program in the **Service** section of the main window (see fig. 65).



Figure 65. Information on the program, the license, and the system it is installed on

All the information is broken into three sections:

- The program version, the date of the last update, and the number of threats known to date are displayed in the **Product info** box.
- Basic information on the operation system installed on your computer is shown in the **System info** box.
- Basic information about the license you purchased for Kaspersky Anti-Virus is contained in the **License info** box.

You will need all this information when you contact Kaspersky Lab Technical Support (see 14.5 on pg. 168).

14.5. Managing licenses

Kaspersky Anti-Virus needs a *license key* to operate. You are provided with a key when you buy the program. It gives you the right to use the program from the day you install the key.

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

If a trial version of the program has been activated (good for thirty days), after the trial period expires, Kaspersky Anti-Virus will not run.

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

To avoid infecting your computer with new viruses, we recommend extending your Kaspersky Anti-Virus license. The program will notify you two weeks prior to the expiration of your license, and for the next two weeks it will display this message every time you open it.

To extend your license, you must purchase and install a new license key for Kaspersky Anti-Virus or enter a program activation code. To do so:

1. Contact the vendor where you purchased the product and purchase an activation code.

or.

Purchase a license key or activation code directly from Kaspersky Lab by clicking the [Purchase license](#) link in the license key window. Complete the form on our website. After payment is made, we will send a link to the e-mail address you enter in the order form. With this link, you can download a license key or receive a program activation code.



Figure 66. License info

Kaspersky Lab regularly has special pricing offers on license extensions for our products. Check for specials on the Kaspersky Lab website in the **Products → Sales and special offers** area.

Information about the license key used is available in the **License info** box in the **Service** section of the main program window. To open the license manager window, left-click anywhere in the box. In the window that opens (see Figure 66), you can view information on the current key, add a key, or delete a key.

When you select a key from the list in the **License info** box, information will be displayed on the license number, type, and expiration date. To add a new license key, click **Add** and activate the application with the activation wizard (see 3.2.2 on pg. 31). To delete a key from the list, use the **Delete** button.

To review the terms of the EULA, click the [View EULA](#) link. To purchase a license through the e-store on the Kaspersky Lab website, click the [Purchase license](#) link.

14.6. Technical Support

Kaspersky Anti-Virus provides you with a wide range of options for questions and problems related to program operation. They are all located in **Support** (see fig. 67) in the **Service** section.



Figure 67. Technical support information

Depending on the problem, we provide several technical support services:

User forum. This resource is a dedicated section of the Kaspersky Lab website with questions, comments, and suggestions by program users. You can look through the basic topics of the forum and leave a comment yourself. You also might find the answer to your question.

To access this resource, use the [User forum](#) link.

Knowledge Base. This resource is also a dedicated section of the Kaspersky Lab website and contains Technical Support recommendations for using Kaspersky Lab software and answers to frequently asked questions. Try to find an answer to your question or a solution to your problem with this resource.

To obtain technical support online, click the [Knowledge Base](#) link.

Comments on program operation. This service is designed for posting comments on program operation or describing a problem that surfaced in program operation. You must fill out a special form on the company's website that describes the situation in detail. In order to best deal with the problem, Kaspersky Lab will need some information about your system. You can describe the system configuration on your own or use the automatic information collector on your computer.

To go to the comment form, use the [Tell about this error or leave a comment about the program](#) link.

Technical support. If you need help with using Kaspersky Anti-Virus, click the link located in the **Local Support Service** box. The Kaspersky Lab website will then open with information about how to contact our specialists.

14.7. Creating a monitored port list

Components such as Mail Anti-Virus, Web Anti-Virus monitor data streams that are transmitted using certain protocols and pass through certain open ports on your computer. Thus, for example, Mail Anti-Virus analyzes information transferred using SMTP protocol, and Web Anti-Virus analyzes information transferred using HTTP.

The standard list of ports that are usually used for transmitting email and HTTP traffic is included in the program package. You can add a new port or disable monitoring for a certain port, thereby disabling dangerous object detection for traffic passing through that port.

To edit the monitored port list, take the following steps:

1. Open the Kaspersky Anti-Virus settings window by clicking the [Settings](#) link in the main window.
2. Select **Network settings** in the **Service** section of the program settings tree.
3. In the right-hand part of the settings window, click **Port settings**.
4. Edit the list of the monitored ports in the window that opens (see fig. 68).

This window provides a list of ports monitored by Kaspersky Anti-Virus. To scan data streams enter on all open network ports, select the option **Monitor all ports**. To edit the list of monitored ports manually, select **Monitor selected ports only**.

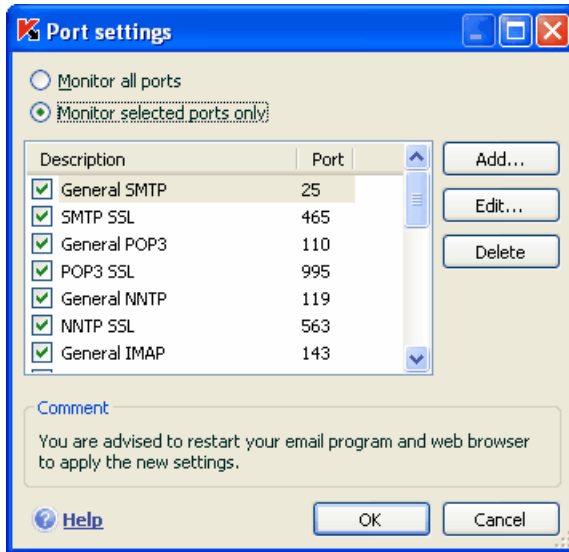


Figure 68. List of monitored ports

To add a new port to the monitored port list:

1. Click on the **Add** button in the **Port settings** window.
2. Enter the port number and a description of it in the appropriate fields in the **New Port** window.

For example, there might be a nonstandard port on your computer through which data is being exchanged with a remote computer using the HTTP protocol, which is monitored by Web Anti-Virus. To analyze this traffic for malicious code, you can add this port to a list of controlled ports.

When any of its components starts, Kaspersky Anti-Virus opens port 1110 as a listening port for all incoming connections. If that port is busy at the time, it selects 1111, 1112, etc. as a listening port.

If you use Kaspersky Anti-Virus and another company's firewall simultaneously, you must configure that firewall to allow the *avp.exe* process (the internal Kaspersky Anti-Virus process) access to all the ports listed above.

For example, say your firewall contains a rule for *iexplorer.exe* that allows that process to establish connections on port 80.

However, when Kaspersky Anti-Virus intercepts the connection query initiated by *iexplorer.exe* on port 80, it transfers it to *avp.exe*, which in turn attempts to establish a connection with the web page independently. If there is no allow rule

for *avp.exe*, the firewall will block that query. The user will then be unable to access the webpage.

14.8. Checking your SSL connection

Connecting using SSL protocol protects data exchange through the Internet. SSL protocol can identify the parties exchanging data using electronic certificates, encode the data being transferred, and ensure their integrity during the transfer.

These features of the protocol are used by hackers to spread malicious programs, since most antivirus programs do not scan SSL traffic.

Kaspersky Anti-Virus 6.0 has the option of scanning SSL traffic for viruses. When an attempt is made to connect securely to a web resource, a notification will appear on screen (see Figure 69) prompting the user for action.

The notification contains information on the program initiating the secure connection, along with the remote address and port. The program asks you to decide whether that connection should be scanned for viruses:

- **Process** – scan traffic for viruses when connecting securely to the website.

We recommend that you always scan SSL traffic if you are using a suspicious website or if an SSL data transfer begins when you go to the next page. It is quite likely that this is a sign of a malicious program being transferred over secure protocol.

- **Skip** – continue secure connection with the website without scanning traffic for viruses.

To apply the action selected in the future to all attempts to establish SSL connections, check **Apply to all**.



Figure 69. Notification on SSL connection detection

To scan encrypted connections, Kaspersky Anti-Virus replaces the security certificate requested with a certificate it signs itself. In some cases, programs that are establishing connections will not accept this certificate, resulting in no connection being established. We recommend disabling SSL traffic scanning in the following cases:

- When connecting to a trusted web resource, such as your bank's web page, where you manage your personal account. In this case, it is important to receive confirmation of the authenticity of the bank's certificate.
- If the program establishing the connection checks the certificate of the website being accessed. For example, MSN Messenger checks the authenticity of the Microsoft Corporation digital signature when it establishes a connection with the server.

You can configure SSL scan settings on the **Network settings** tab of the program settings window:

Check all encrypted connections – scan all traffic incoming on SSL protocol for viruses.

Prompt user when a new encrypted connection is detected – display a message prompting the user for action every time an SSL connection is established.

Do not check encrypted connections – do not scan traffic incoming on SSL protocol for viruses.

14.9. Configuring the Kaspersky Anti-Virus interface

Kaspersky Anti-Virus gives you the option of changing the appearance of the program by creating and using skins. You can also configure the use of active interface elements such as the system tray icon and popup messages.

To configure the program interface, take the following steps:

1. Open the Kaspersky Anti-Virus settings window by clicking the [Settings](#) link in the main window.
2. Select **Appearance** in the **Service** section of the program settings tree (see fig. 70).

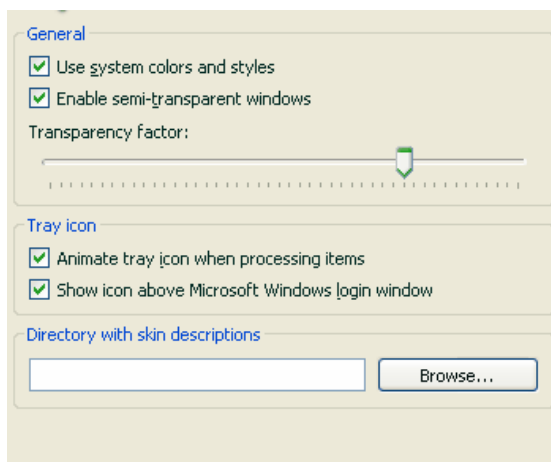


Figure 70. Configuring program appearance settings

In the right-hand part of the settings window, you can determine:

- Whether to display the Kaspersky Anti-Virus protection indicator when the operating system starts.

This indicator by default appears in the upper right-hand corner of the screen when the program loads. It informs you that your computer is protected from all threat types. If you do not want to use the protection indicator, uncheck **Show icon above Microsoft Windows login window**.

- Whether to use animation in the system tray icon.

Depending on the program operation performed, the system tray icon changes. For example, if a script is being scanned, a small depiction of a script appears in the background of the icon, and if an email is being scanned, an envelope. By default, icon animation is enabled. If you want to turn off animation, uncheck **Animate tray icon when processing items**. Then the icon will only reflect the protection status of your computer: if protection is enabled, the icon is in color, and if protection is paused or disabled, the icon becomes gray.

- Degree of transparency of popup messages.

All Kaspersky Anti-Virus operations that must immediately reach you or require you to make a decision are presented as popup messages above the system tray icon. The message windows are transparent so as not to interfere with your work. If you move the cursor over the message, the transparency disappears. You can change the degree of transparency of such messages. To do so, adjust the **Transparency factor** scale to the desired position. To remove message transparency, uncheck **Enable semi-transparent windows**.

This option is not available if you are running the application under Microsoft Windows 98/NT 4.0/ME.

- Use your own skins for the program interface.

All the colors, fonts, icons, and texts used in the Kaspersky Anti-Virus interface can be changed. You can create your own graphics for the program or can localize it in another language. To use a skin, specify the directory with its settings in the **Directory with skin descriptions** field. Use the **Browse** button to select the directory.

By default, the system colors and styles are used in the program's skin. You can remove them by deselecting **Use system colors and styles**. Then the styles that you specify in the screen theme settings will be used.

Note that changes to Kaspersky Anti-Virus interface settings are not saved if you restore default operation settings or uninstall the program.

14.10. Rescue Disk

Kaspersky Anti-Virus has a tool for creating a rescue disk.

The rescue disk is designed to restore system functionality after a virus attack that has damaged system files and made the operating system impossible to start. This disk includes:

- Microsoft Windows XP Service Pack 2 system files
- A set of operating system diagnostic utilities
- Kaspersky Anti-Virus program files
- Files containing threat signatures

To create a rescue disk:

1. Open the program's main window and select **Rescue disk** in the **Service** section.
2. Click the **Start Wizard** button to begin creating the rescue disk.

A Rescue Disk is designed for the computer that it was created on. Using the disk on other computers could lead to unforeseeable consequences, since it contains information about the parameters of a specific computer (info on boot sectors, for example).

You can only create a rescue disk under Windows XP or Microsoft Windows Vista. The rescue disk feature is not available under other supported operating systems, including Microsoft Windows XP Professional x64 Edition and Microsoft Windows Vista x64.

14.10.1. Creating a rescue disk

Warning! You will need the Microsoft Windows XP Service Pack 2 installation disk to create an emergency disk.

You need the program **PE Builder** to create the Rescue Disk.

You must install these PE Builder on your computer beforehand to create an emergency disk with it.

A special Wizard walks you through the creation of a rescue disk. It consists of a series of windows/steps which you can navigate using the **Back** and **Next** buttons. You can complete the Wizard by clicking **Finished**. The **Cancel** button will stop the Wizard at any point.

14.10.1.1. Getting ready to write the disk

To create a rescue disk, specify the path to the following folders:

- PE Builder program folder
- Folder where rescue disk files will be saved before burning the CD

If you are not creating an emergency disk for the first time, this folder will already contain a set of files made the last time. To use files saved previously, check the corresponding box.

Note that a previous version of the rescue disk files will contain outdated threat signatures. To optimally analyze the computer for viruses and to restore the system, we recommend updating threat signatures and creating a new version of the rescue disk.

- The Microsoft Windows XP Service Pack 2 installation CD

After entering the paths to the folders required, click **Next**. PE Builder will start up and the rescue disk creation process will begin. Wait until the process is complete. This could take several minutes.

14.10.1.2. Creating an .iso file

After PE Builder has completed creating the rescue disk files, a **Create .iso file** window will open.

The .iso file is a CD image of the rescue disk, saved as an archive. The majority of CD burning programs correctly recognize .iso files (Nero, for example).

If this is not the first time that you have created a rescue disk, you can select the .iso file from the previous disk. To do so, select **Existing .iso file**.

14.10.1.3. Burning the disk

This Wizard window will ask you to choose whether to burn the rescue disk files to CD now or later.

If you chose to burn the disk right away, specify whether you want to format the CD before burning. To do so, check the corresponding box. You only have this option if you are using a CD-RW.

The CD will start burning when you click the **Next** button. Wait until the process is complete. This could take several minutes.

14.10.1.4. Finishing creating a rescue disk

This Wizard window informs you that you have successfully created a rescue disk.

14.10.2. Using the rescue disk

Note that Kaspersky Anti-Virus only works in system rescue mode if the main

window is opened. When you close the main window, the program will close.

Bart PE, the default program, does not support .chm files or Internet browsers, so you will not be able to view Kaspersky Anti-Virus Help or links in the program interface while in Rescue Mode.

If a situation arises when a virus attack makes it impossible to load the operating system, take the following steps:

1. Create an emergency boot disk by using Kaspersky Anti-Virus on an uninfected computer.
2. Insert the emergency disk in the disk drive of the infected computer and restart. Microsoft Windows XP SP2 will start with the Bart PE interface. Bart PE has built-in network support for using your LAN. When the program starts, it will ask you if you want to enable it. You should enable network support if you plan to update threat signatures from the LAN before scanning your computer. If you do not need to update, cancel network support.
3. To open Kaspersky Anti-Virus, click **Start → Programs → Kaspersky Anti-Virus 6.0 → Start**.

The Kaspersky Anti-Virus main window will open. In system rescue mode, you can only access virus scans and threat signature updates from the LAN (if you have enabled network support in Bart PE).

4. Start the virus scan.

Note that threat signatures from the date that the rescue disk is created are used by default. For this reason, we recommend updating threat signatures before starting the scan.

It should also be noted that the application will only use the updated Threat Signatures during the current session with the rescue disk, prior to restarting your computer.

Warning! If infected or potentially infected objects were detected when you scanned the computer, and they were processed and then moved to Quarantine or Backup Storage, we recommend completing processing those objects during the current session with a rescue disk.

Otherwise, these objects will be lost when you restart your computer.

14.11. Using advanced options

Kaspersky Anti-Virus provides you with the following advanced features:

- Notifications of certain events that occur in the program.
- Kaspersky Anti-Virus Self-Defense against modules being disabled, deleted, or edited, as well as password protection for the program.
- Resolving conflicts with Kaspersky Anti-Virus (see 14.11.3 on pg. 187) when using other applications.

To configure these features:

1. Open the program setup window with the Settings link in the main window.
2. Select **Service** from the settings tree.

In the right hand part of the screen you can define whether to use additional features in program operation.

14.11.1. Kaspersky Anti-Virus event notifications

Different kinds of events occur in Kaspersky Anti-Virus. They can be of an informative nature or contain important information. For example, an event can inform you that the program has updated successfully, or can record an error in a component that must be immediately eliminated.

To receive updates on Kaspersky Anti-Virus operation, you can use the notification feature.

Notices can be delivered in several ways:

- Popup messages above the program icon in the system tray
- Sound messages
- Emails
- Logging events

To use this feature, you must:

1. Check **Enable notifications** in the **Interaction with user** box (see fig. 71).

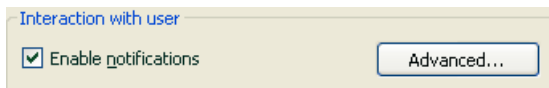


Figure 71. Enabling notifications

2. Click on the **Settings** button to open the **Notification settings** window.
3. On the **Events** tab, define the event types from Kaspersky Anti-Virus for which you want notifications, and the notification delivery method (see 14.11.1.1 on pg. 181).
4. Click **Email Settings** to open **Notification Settings** window to configure email notification delivery settings, if that is the notification method that is being used (see 14.11.1.2 on pg. 183).

14.11.1.1. Types of events and notification delivery methods

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

Critical notifications are events of a critical importance. Notifications are highly recommended, since they point to problems in program operation or vulnerabilities in protection on your computer. For example, *threat signatures corrupt* or *license expired*.

Functional failure – events that lead to the application not working. For example, no license or threat signatures.

Important notifications are events that must be investigated, since they reflect important situations in the operation of the program. For example, *protection disabled* or *computer has not been scanned for viruses for a long time*.

Minor notifications are reference-type messages which generally do not contain important information. For example, *all dangerous objects disinfected*.

To specify which events the program should notify you of and how:

1. Click the Settings link in the program's main window.
2. In the program settings window, select **Service**, check **Enable notifications**, and edit detailed settings by clicking the **Advanced** button.

You can configure the following notification methods for the events listed above in the **Notification settings** window that opens (see fig. 72):

- *Popup messages* above the program icon in the system tray that contain an informative message on the event that occurred.

To use this notification type, check in the **Balloon** section across from the event about which you want to be informed.

- *Sound notification*

If you want this notice to be accompanied by a sound, check **Sound** across from the event.

- *Email notification*

To use this type of notice, check the **Email** column across from the event about which you want to be informed, and configure settings for sending notices (see 14.11.1.2 on pg. 183).

- *Logging events*

To record information in the log about events that occur, check in the **Log** column and configure event log settings (see 14.11.1.3 on pg. 184).

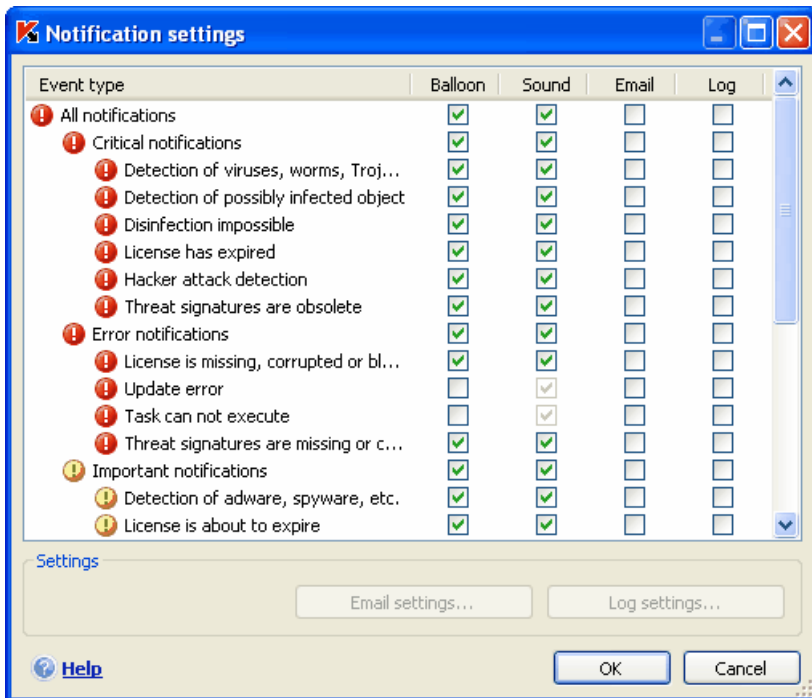


Figure 72. Program events and event notification methods

14.11.1.2. Configuring email notification

After you have selected the events (see 14.11.1.1 on pg. 181) about which you wish to receive email notifications, you must set up notification delivery. To do so:

1. Open the program setup window with the [Settings](#) link in the main window.
2. Select **Service** in the settings tree.
3. Click **Advanced** in the **Interaction with user** section of the right-hand part of the screen.
4. In the **Notification settings** window, select the checkbox in the **Email** chart for events that should trigger an e-mail message.
5. In the window (see fig. 73) that opens when you click **Email settings**, configure the following settings for sending e-mail notifications:
 - Assign the sending notification setting for **From: Email address**.
 - Specify the email address to which notices will be sent in **To: Email address**.
 - Assign a email notification delivery method in the **Send mode**. If you want the program to send email as soon as the event occurs, select **Immediately when event occurs**. For notifications about events within a certain period of time, fill out the schedule for sending informative emails by click **Edit**. Daily notices are the default.

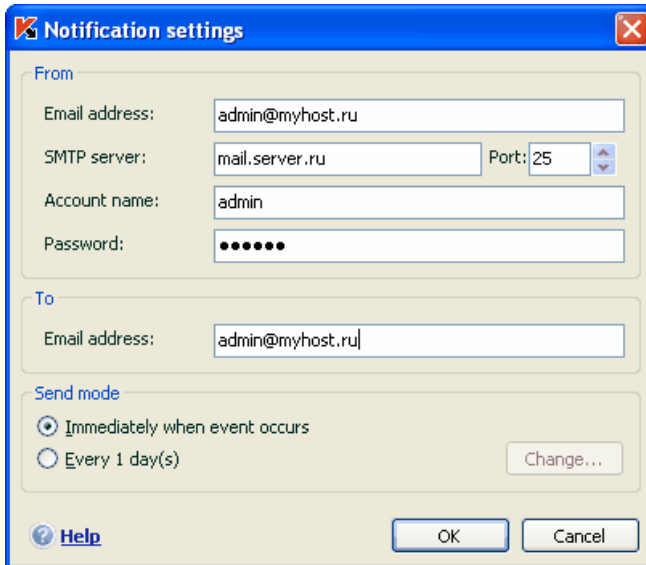


Figure 73. Configuring email notification settings

14.11.1.3. Configuring event log settings

To configure event log settings:

1. Open the application settings window with the [Settings](#) link in the main window.
2. Select **Service** in the settings tree.
3. Click **Advanced** in the **Interaction with user** section of the right-hand part of the screen.

In the **Notification settings** window, select the option of logging information for an event and click the **Log Settings** button.

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

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

You cannot log events under Microsoft Windows 98/ME, and you cannot log to the **Kaspersky Event Log** under Microsoft Windows NT 4.0.

These limitations are because of the particulars of these operating systems.

14.11.2. Self-Defense and access restriction

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

Moreover, several people may be using the same computer, all with varying levels of computer literacy. Leaving access to the program and its settings open could dramatically lower the security of the computer as a whole.

To ensure the stability of your computer's security system, Self-Defense, remote access defense, and password protection mechanisms have been added to the program.

Application self-defense is not available if Kaspersky Anti-Virus is installed under Microsoft Windows 98/ME/XP Professional x64 Edition.

On computers running 64-bit operating systems and Microsoft Windows Vista, self-defense is only available for preventing the program's own files on local drives and system registry records from being modified or deleted.

To enable Self-Defense:

1. Open the program settings window with the [Settings](#) link in the main window.
2. Select **Service** from the settings tree.
3. Make the following configurations in the **Self-Defense** box (see fig. 74):

Enable Self-Defense. If this box is checked, the program will protect its own files, processes in memory, and entries in the system registry from being deleted or modified.

Disable external service control. If this box is checked, any remote administration program attempting to use the program will be blocked.

If any of the actions listed are attempted, a message will appear over the program icon in the system tray (if the notification service has not been disabled by the user).

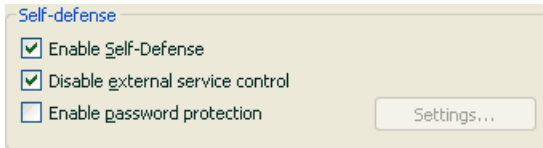


Figure 74. Configuring program defense

To password-protect the program, check **Enable password protection**. Click on the **Settings** button to open the **Password protection** window, and enter the password and area that the access restriction will cover (see fig. 75). You can block any program operations, except notifications for dangerous object detection, or prevent any of the following actions from being performed:

- Change of program performance settings
- Close Kaspersky Anti-Virus
- Disable or pause protection on your computer

Each of these actions lowers the level of protection on your computer, so try to establish which of the users on your computer you trust to take such actions.

Now whenever any user on your computer attempts to perform the actions you selected, the program will request a password.

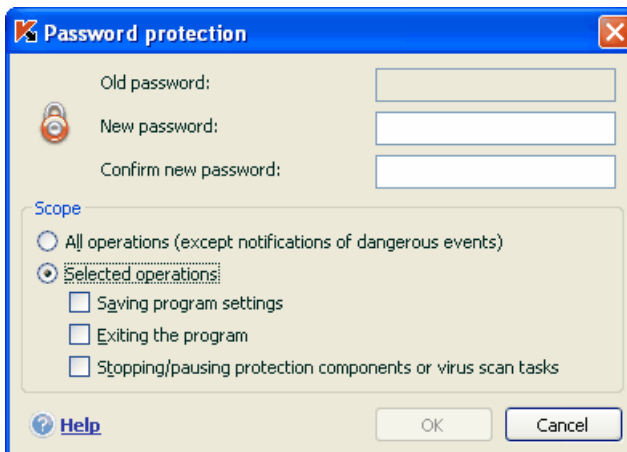


Figure 75. Program password protection settings

14.11.3. Resolving conflicts with other applications

In some cases, Kaspersky Anti-Virus may cause conflicts with other applications installed on a computer. This is because those programs have built-in self-defense mechanisms that turn on when Kaspersky Anti-Virus attempts to inspect them. These applications include the Authentica plug-in for Acrobat Reader, which verifies access to .pdf files, Oxygen Phone Manager II, and some computer games that have digital rights management tools.

To fix this problem, check **Compatibility mode for programs using self-protection methods** in the **Service** section of the application settings window. You must restart your operating system for this change to take effect.

However, note that if you select the checkbox, Office Guard will not work. If you enable Office Guard, compatibility with application self-defense will be disabled automatically. Once enabled, macro scans will begin running once you restart the operating system.

14.12. Importing and exporting Kaspersky Anti-Virus settings

Kaspersky Anti-Virus allows you to import and export settings.

This feature is useful when, for example, the program is installed both on your home computer and in your office. You can configure the program the way you want it at home, save those settings on a disk, and using the import feature, load them on your computer at work. The settings are saved in a special configuration file.

To export the current program settings:

1. Open the Kaspersky Anti-Virus main window.
2. Select the **Service** section and click Settings.
3. Click the **Save** button in the **Configuration Manager** section.
4. Enter a name for the configuration file and select a save destination.

To import settings from a configuration file:

1. Open the Kaspersky Anti-Virus main window.
2. Select the **Service** section and click Settings.

3. Click the **Load** button and select the file from which you want to import Kaspersky Anti-Virus settings.

14.13. Resetting to default settings

It is always possible to return to the default program settings, which are considered the optimum and are recommended by Kaspersky Lab. This can be done using the Setup Wizard.

To reset protection settings:

1. Select the **Service** section and click Settings to go to the program configuration window.
2. Click the **Reset** button in the **Settings Manager** section.

The window that opens asks you to define which settings should be restored to their default values.

The window lists the program components whose settings were changed by the user. If special settings were created for any of the components, they will also be shown on the list.

Examples of special settings are:; trusted address lists used by Web Anti-Virus; exclusion rules created for program components and application rules for Proactive Defense.

These lists are populated gradually by using the program, based on individual tasks and security requirements. This process often takes some time. Therefore, we recommend saving them when you reset program settings.

The program saves all the custom settings on the list by default (they are unchecked). If you do not need to save one of the settings, check the box next to it.

After you have finished configuring the settings, click the **Next** button. Setup Wizard will open. Follow its instructions.

After you are finished with the Setup Wizard, the **Recommended** security level will be set for all components, except for the settings that you decided to keep. In addition, settings that you configured with the Setup Wizard will also be applied.

CHAPTER 15. WORKING WITH THE PROGRAM FROM THE COMMAND PROMPT

You can use Kaspersky Anti-Virus from the command prompt. You can execute the following operations:

- Starting, stopping, pausing and resuming the activity of application components
- Starting, stopping, pausing and resuming virus scans
- Obtaining information on the current status of components, tasks and statistics on them
- Scanning selected objects
- Updating threat signatures and program modules
- Accessing Help for command prompt syntax
- Accessing Help for command syntax

The command prompt syntax is:

```
avp.com <command> [settings]
```

The following may be used as **<commands>**:

| | |
|-----------------|---|
| ACTIVATE | Activates application via Internet using an activation code |
| ADDKEY | Activates application using a license key file |
| START | Starts a component or a task |
| PAUSE | Pauses a component or a task |
| RESUME | Resumes a component or a task |
| STOP | Stops a component or a task |
| STATUS | Displays the current component or task status on |

| | |
|-------------------|--|
| | screen |
| STATISTICS | Displays statistics for the component or task on screen |
| HELP | Help with command syntax and the list of commands |
| SCAN | Scans objects for viruses |
| UPDATE | Begins program update |
| ROLLBACK | Rolls back to the last program update made |
| EXIT | Closes the program (you can only execute this command with the password assigned in the program interface) |
| IMPORT | Import application settings |
| EXPORT | Export application settings |

Each command uses its own settings specific to that particular Kaspersky Anti-Virus component.

15.1. Activating the application

You can activate the program in two ways:

- via Internet using an activation code (the **ACTIVATE** command)
- using a license key file (the **ADDKEY** command)

Command syntax:

```
ACTIVATE <activation_code>  
ADDKEY <file_name>
```

Parameter description:

| | |
|--------------------------------------|---|
| <code><activation_code></code> | Program activation code provided when you purchased it. |
| <code><file_name></code> | Name of the license key file with the extension *.key. |

Example:

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key
```

15.2. Managing program components and tasks

You can manage Kaspersky Anti-Virus components and tasks from the command prompt with these commands:

- START
- PAUSE
- RESUME
- STOP
- STATUS
- STATISTICS

The task or component to which the command applies is determined by its parameter.

STOP and PAUSE can only be executed with the Kaspersky Anti-Virus password assigned in the program interface.

Command syntax:

```
avp.com <command> <profile|taskid>
avp.com STOP
PAUSE <profile|taskid> /password=<password>
```

One of the following values is assigned to `<profile|taskid>`:

| | |
|------------|---------------------------|
| RTP | All protection components |
|------------|---------------------------|

| | |
|----------------------------|----------------------|
| FM | File Anti-Virus |
| EM | Mail Anti-Virus |
| WM | Web Anti-Virus |
| BM | Proactive Defense |
| UPDATER | Updater |
| SCAN_OBJECTS | Virus scan task |
| SCAN_MY_COMPUTER | My Computer task |
| SCAN_CRITICAL_AREAS | Critical Areas task |
| SCAN_STARTUP | Startup Objects task |
| <task name> | User-defined task |

Components and tasks started from the command prompt are run with the settings configured with the program interface.

Examples:

To enable File Anti-Virus, type this at the command prompt:

```
avp.com START FM
```

To view the current status of Proactive Defense on your computer, type the following text at the command prompt:

```
avp.com STATUS BM
```

To stop a My Computer scan task from the command prompt, enter:

```
avp.com STOP SCAN_MY_COMPUTER  
/password=<your_password>
```

15.3. Anti-virus scans

The syntax for starting a virus scan of a certain area, and processing malicious objects, from the command prompt generally looks as follows:

```
avp.com SCAN [<object scanned>] [<action>] [<action  
query>] [<file types>] [<exclusions>] [<configuration  
file>] [<report settings>]
```

To scan objects, you can also start one of the tasks created in Kaspersky Anti-Virus from the command prompt (see 15.1 on pg. 190). The task will be run with the settings specified in the program interface.

Parameter description.

| | |
|---|--|
| <p><object scanned> - this parameter gives the list of objects that will be scanned for malicious code.</p> <p>It can include several values from the following list, separated by spaces.</p> | |
| <files> | <p>List of paths to the files and/or folders to be scanned. You can enter absolute or relative paths. Items in the list are separated by a space.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If the object name contains a space, it must be placed in quotation marks • If you select a specific folder, all the files in it are scanned. |
| /MEMORY | System memory objects |
| /STARTUP | Startup objects |
| /MAIL | Email databases |
| /REMDRIVES | All removable media drives |
| /FIXDRIVES | All internal drives |
| /NETDRIVES | All network drives |
| /QUARANTINE | Quarantined objects |
| /ALL | Complete scan |
| /@:<filelist.lst> | <p>Path to a file containing a list of objects and folders to be included in the scan. The file should be in a text format and each scan object must start a new line.</p> <p>You can enter an absolute or relative path to the file. The path must be placed in quotation marks if it contains a space.</p> |

| | |
|--|--|
| <action> - this parameter sets responses to malicious objects detected during the scan. If this parameter is not defined, the default value is <code>/i2</code> . | |
| <code>/i0</code> | take no action on the object; simply record information about it in the report. |
| <code>/i1</code> | Treat infected objects, and if disinfection fails, skip |
| <code>/i2</code> | Treat infected objects, and if disinfection fails, delete. Exceptions: do not delete infected objects from compound objects; delete compound objects with executable headers, i.e. sfx archives (default). |
| <code>/i3</code> | Treat infected objects, and if disinfection fails, delete. Also delete all compound objects completely if infected contents cannot be deleted. |
| <code>/i4</code> | Delete infected objects, and if disinfection fails, delete. Also delete all compound objects completely if infected contents cannot be deleted. |
| <action query> - this parameter defines which actions will prompt the user for a response during the scan. If the parameter is not defined, the default value is <code>/a2</code> . | |
| <code>/i8</code> | Prompt the user for action if an infected object is detected. |
| <code>/i9</code> | Prompt the user for action at the end of the scan. |
| <file types> - this parameter defines the file types that will be subject to the anti-virus scan. If this parameter is not defined, the default value is <code>/fi</code> . | |
| <code>/fe</code> | Scan only potentially infected files by extension |
| <code>/fi</code> | Scan only potentially infected files by contents (default) |
| <code>/fa</code> | Scan all files |

| | |
|--|---|
| <p><exclusions> - this parameter defines objects that are excluded from the scan.</p> <p>It can include several values from the list provided, separated by spaces.</p> | |
| /e:a | Do not scan archives |
| /e:b | Do not scan email databases |
| /e:m | Do not scan plain text emails |
| /e:<mask> | Do not scan objects by mask |
| /e:<seconds> | Skip objects that are scanned for longer that the time specified in the <seconds> parameter. |
| /es:<size> | Skip files larger (in MB) than the value assigned by <size> . |
| <p><configuration file> - defines the path to the configuration file that contains the program settings for the scan.</p> <p>You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the Kaspersky Anti-Virus interface are used.</p> | |
| /C:<settings_file> | Use the settings values assigned in the file <settings_file> |
| <p><report settings> - this parameter determines the format of the report on scan results.</p> <p>You can use an absolute or relative path to the file. If the parameter is not defined, the scan results are displayed on screen, and all events are displayed.</p> | |
| /R:<report_file> | Only log important events in this file |
| /RA:<report_file> | Log all events in this file |

Examples:

Start a scan of RAM, Startup programs, email databases, the directories **My Documents** and **Program Files**, and the file **test.exe**:

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Pause scan of selected objects and start full computer scan, then continue to scan for viruses within the selected objects:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Scan RAM and the objects listed in the file **object2scan.txt**. Use the configuration file **scan_setting.txt**. After the scan, generate a report in which all events are recorded:

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

15.4. Program updates

The syntax for updating Kaspersky Anti-Virus program modules and threat signatures from the command prompt is as follows:

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP]
```

Parameter description:

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

| | |
|---------------------------------------|---|
| <code>/C:<settings_file></code> | <p>Path to the configuration file with the settings for program updates.</p> <p>You can enter an absolute or relative path to the file. If this parameter is not defined, the values for the settings in the Kaspersky Anti-Virus interface are used.</p> |
| <code>/APP</code> | Update program modules |

Examples:

Update threat signatures and record all events in the report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update the Kaspersky Anti-Virus program modules by using the settings in the configuration file **updateapp.ini**:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

15.5. Rollback settings

Command syntax:

```
ROLLBACK [/R[A]:<report_file>]
```

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

Example:

```
avp.com ROLLBACK /RA:rollback.txt
```

15.6. Exporting settings

Command syntax:

```
avp.com EXPORT <profile|taskid> <filename>
```

Parameter description:

| | |
|-------------------------|---|
| <profile> | <p>Component or task with the settings being exported.</p> <p>One of the following values may be used:</p> <p>RTP – all protection components</p> <p>FM – File Anti-Virus</p> <p>EM – Mail Anti-Virus</p> <p>WM – Web Anti-Virus</p> <p>BM - Proactive Defense</p> |
| <filename> | <p>Path to the file to which the Kaspersky Anti-Virus settings are exported. You can use an absolute or relative path.</p> <p>The configuration file is saved in binary format (<i>.dat</i>), and it can be used later to import application settings on other computers. The configuration file can be saved as a text file. To do so, specify the <i>.txt</i> extension in the file name.</p> |

Example:

```
avp.com EXPORT c:\settings.dat
```

15.7. Importing settings

Command syntax:

```
avp.com IMPORT <filename> [/password=<password>]
```

| | |
|-------------------------|--|
| <filename> | <p>Path to the file from which the Kaspersky Anti-Virus settings are being imported. You can use an absolute or relative path.</p> |
| <password> | <p>Password to Kaspersky Anti-Virus assigned in the application interface.</p> |

Note that this command cannot be executed without the password.

Example:

```
avp.com IMPORT c:\ settings.dat /password=<your_password>
```

15.8. Starting the program

Command syntax:

```
avp.com
```

15.9. Stopping the program

Command syntax:

```
EXIT /password=<password>
```

| | |
|------------|--|
| <password> | Kaspersky Anti-Virus password assigned in the program interface. |
|------------|--|

Note that you cannot execute this command without entering the password.

15.10. Viewing Help

This command is available for viewing Help on command prompt syntax:

```
avp.com [ /? | HELP ]
```

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

```
avp.com <command> /?
```

```
avp.com HELP <command>
```

15.11. Return codes from the command line interface

This section contains a list of return codes from the command line. The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a specific type of task.

| General return codes | |
|--|----------------------------------|
| 0 | Operation completed successfully |
| 1 | Invalid setting value |
| 2 | Unknown error |
| 3 | Task completion error |
| 4 | Task canceled |
| Anti-virus scan task return codes | |
| 101 | All dangerous objects processed |
| 102 | Dangerous objects detected |

CHAPTER 16. MODIFYING, REPAIRING, AND REMOVING THE PROGRAM

You can uninstall the application in the following ways:

- Using the Setup Wizard (see 16.1 on pg. 201)
- From the command prompt (see 16.2 on pg. 203)

16.1. Modifying, repairing and removing the program using Setup Wizard

You may find it necessary to repair the program if you detect errors in its operation after incorrect configuration or file corruption.

Modifying the program can install missing Kaspersky Anti-Virus components and delete unwanted ones.

To repair or modify Kaspersky Anti-Virus missing components or delete the program:

1. Exit the program. To do so, left-click on the program icon in the system tray and select **Exit** from the context menu.
2. Insert the installation CD into the CD-ROM drive, if you used one to install the program. If you installed Kaspersky Anti-Virus from a different source (public access folder, folder on the hard drive, etc.), make sure that the installer package is in the folder and that you have access to it.
3. Select **Start → Programs → Kaspersky Anti-Virus 6.0 for Windows Workstations → Modify, Repair, or Remove**.

An installation wizard then will open for the program. Let's take a closer look at the steps of repairing, modifying, or deleting the program.

Step 1. Installation Welcome window

If you take all the steps described above necessary to repair or modify the program, the Kaspersky Anti-Virus installation welcome window will appear. To continue, click the **Next** button.

Step 2. Selecting an operation

At this stage, you select which operation you want to run. You can modify the program components, repair the installed components, remove components or remove the entire program. To execute the operation you need, click the appropriate button. The program's response depends on the operation you select.

Modifying the program is like custom program installation where you can specify which components you want to install, and which you want to delete.

Repairing the program depends on the program components installed. The files will be repaired for all components that are installed and the Recommended security level will be set for each of them.

If you remove the program, you can select which data created and used by the program you want to save on your computer. To delete all Kaspersky Anti-Virus data, select **Complete uninstall**. To save data, select **Save application objects** and specify which objects not to delete from this list:

- *Activation data* – license key or program activation code.
- *Threat signatures* – complete set of signatures of dangerous programs, virus, and other threats current as of the last update.
- *Backup files* – backup copies of deleted or disinfected objects. You are advised to save these, in case they can be restored later.
- *Quarantine files* – files that are potentially infected by viruses or modifications of them. These files contain code that is similar to code of a known virus but it is difficult to determine if they are malicious. You are advised to save them, since they could actually not be infected, or they could be disinfected after the threat signatures are updated.
- *Application settings* – configurations for all program components.
- *iSwift data* – database with information on objects scanned on NTFS file systems, which can increase scan speed. When it uses this database, Kaspersky Anti-Virus only scans the files that have been modified since the last scan.

Warning!

If a long period of time elapses between uninstalling one version of Kaspersky Anti-Virus and installing another, you are advised not to use the *iSwift* database from a previous installation. A dangerous program could penetrate the computer during this period and its effects would not be detected by the database, which could lead to an infection.

To start the operation selected, click the **Next** button. The program will begin copying the necessary files to your computer or deleting the selected components and data.

Step 3. Completing program modification, repair, or removal

The modification, repair, or removal process will be displayed on screen, after which you will be informed of its completion.

Removing the program generally requires you to restart your computer, since this is necessary to account for modifications to your system. The program will ask if you want to restart your computer. Click **Yes** to restart right away. To restart your computer later, click **No**.

16.2. Uninstalling the program from the command prompt

To uninstall Kaspersky Anti-Virus 6.0 from the command prompt, enter:

```
msiexec /x <package_name>
```

The installation wizard will open. you can use it to uninstall the application (see Chapter 16 on pg. 201).

You can also use the commands given below.

To uninstall the application in the background without restarting the computer (the computer should be restarted manually after uninstalling), enter:

```
msiexec /x <package_name> /qn
```

To uninstall the application in the background and then restart the computer, enter:

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

CHAPTER 17. 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 6.0 with anti-virus products of other vendors?*

No. 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 iStream technologies. The technology is implemented in the program using a database of file checksums and file checksum storage in alternate NTFS streams.

Question: *Why do I need the license key file? Will Kaspersky Anti-Virus work without it?*

Kaspersky Anti-Virus will run without a license key, although you will not be able to access the Updater and Technical Support.

If you still have not decided whether to purchase Kaspersky Anti-Virus, we can provide you with a trial license that will work for either two weeks or a month. Once that time has elapsed, the key will expire.

Question: *After the installation of Kaspersky Anti-Virus the operating system started "behaving" strangely ("blue screen of death", frequent restarting, etc.) What should I do?*

Although rare, it is possible that Kaspersky Anti-Virus and other software installed on your computer will conflict.

In order to restore the functionality of your operating system do the following:

1. Press the **F8** key repeatedly between the time when the computer just started loading until the boot menu is displayed.
2. Select **Safe Mode** and load the operating system.

3. Open Kaspersky Anti-Virus.
4. Use the Settings link in the main window and select the **Protection** section in the program settings window.
5. Uncheck **Run application on system startup** and click **OK**.
6. Reboot the operating system in regular mode.

After this contact the Technical Support Service through the Kaspersky Lab's corporate website (**Services**→**Technical Support**). Describe in detail the problem and the circumstances in which this problem occurs.

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

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


By default, the dump file will be saved into the system folder as *memory.dmp*. You can change the dump storage folder by editing the folder name in the corresponding field.

4. Reproduce the problem related to the operation of Kaspersky Anti-Virus.
5. Make sure that the complete memory dump file was successfully saved.

APPENDIX A. REFERENCE INFORMATION

This appendix contains reference materials on the file formats and extension masks used in Kaspersky Anti-Virus settings.

A.1. List of files scanned by extension

If you select  **Scan programs and documents (by extension)**, File Anti-Virus will scan files with the extensions below in-depth for viruses. Mail Anti-Virus will also scan these files if you enable attachment filtration.

com – executable file for a program

exe – executable file or self-extracting archive

sys – system driver

prg – program text for dBase, Clipper or Microsoft Visual FoxPro, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a .bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic loading library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program that runs in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – initialization file

cla – Java class

vbs – Visual Basic script
vbe – BIOS video extension
js, jse – JavaScript source text
htm – hypertext document
htt – Microsoft Windows hypertext header
hta – hypertext program for Microsoft Internet Explorer
asp – Active Server Pages script
chm – compiled HTML file
pht – HTML with built-in PHP scripts
php – script built into HTML files
wsh – Windows Script Host file
wsf – Microsoft Windows script
the – Microsoft Windows 95 desktop wallpaper
hlp – Win Help file
eml – Microsoft Outlook Express email file
nws – Microsoft Outlook Express new email file
msg – Microsoft Mail email file
plg – email
mbx – extension for saved Microsoft Office Outlook emails
doc – Microsoft Office Word document
dot – Microsoft Office Word document template
fpm – database program, start file for Microsoft Visual FoxPro
rtf – Rich Text Format document
shs – Shell Scrap Object Handler fragment
dwg – AutoCAD blueprint database
msi – Microsoft Windows Installer package
otm – VBA project for Microsoft Office Outlook
pdf – Adobe Acrobat document
swf – Shockwave Flash file
jpg, jpeg – compressed image graphics format
emf – Enhanced Metafile format Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows
ico – icon file
ov? – Microsoft DOC executable files
*xl** – Microsoft Office Excel documents and files, such as: *xla* – Microsoft Office Excel extension, *xlc* – diagram, *xlt* – document templates, etc.

*pp** – Microsoft Office PowerPoint documents and files, such as: *pps* – Microsoft Office PowerPoint slide, *ppt* – presentation, etc.

*md** – Microsoft Office Access documents and files, such as: *mda* – Microsoft Office Access work group, *mdb* – database, etc.

Remember that the actual format of a file may not correspond with the format indicated in the file extension.

A.2. Possible file exclusion masks

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

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

If you do not want the program to scan files in the subfolders of this folder, uncheck **Include subfolders** when creating the mask.

3. Masks with relative file paths:
 - **dir*.*** or **dir*** or **dir** – all files in all *dir* folders
 - **dir\test** – all *test* files in *dir* folders
 - **dir*.exe** – all files with the extension *.exe* in all *dir* folders
 - **dir*.ex?** – all files with the extension *.ex?* in all *C:\dir* folders, where ? can represent any one character

If you do not want the program to scan files in the subfolders of this folder, uncheck **Include subfolders** when creating the mask.

Tip:

. and * exclusion masks can only be used if you assign an excluded threat classification from the Virus Encyclopedia. Otherwise the threat specified will not be detected in any objects. Using these masks without selecting a classification essentially disables monitoring.

We also do not recommend that you select a virtual drive created on the basis of a file system directory using the *subst* command as an exclusion. There is no point in doing so, since during the scan, the program perceives this virtual drive as a folder and consequently scans it.

A.3. Possible threat exclusion classifications from the Virus Encyclopedia

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

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

For some verdicts, you can assign advanced conditions for applying rules in the **Advanced settings** field. In most cases, this field is filled in automatically when you add an exclusion rule from a Proactive Defense notice.

You can add advanced settings for the following verdicts, among others:

- *Invader*. For this verdict, you can give a name, mask, or complete path to the object being embed (for example, a .dll file) as an additional exclusion condition.

Launching Internet Browser. For this verdict, you can list browser open settings as additional exclusion settings.

For example, you blocked browsers from opening with certain settings in the Proactive Defense application activity analysis. However, you want to allow the browser to open for the domain *www.kaspersky.com* with a link from Microsoft

Office Outlook as an exclusion rule. To do so, select Outlook as the exclusion **Object** and Launching Internet Browser as the **Verdict**, and enter an allowed domain mask in the **Advanced settings** field.

APPENDIX B. 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 email 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, email 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.

B.1. Other Kaspersky Lab Products

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 Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, for notifications about the current state of virus activity, and fresh news. The program reads the list of available news channels and their content from the Kaspersky Lab news server at a specified frequency.

The product performs the following functions:

- A system tray icon indicates 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 at the specified frequency and notifies the user of fresh news.
- It allows news on the subscribed channels to be reviewed.
- It allows the list of channels and their status to be edited.
- It allows opening pages with news details in your browser.

News Agent is a stand-alone Microsoft 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 visitors to Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your computer. The Kaspersky OnLine Scanner runs directly in your web browser. Thus, users can quickly test their computers if they suspect a malicious infection. Using the service, visitors can:

- Exclude archives and email databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

Kaspersky® OnLine Scanner Pro

The program is a subscription service offered to visitors to Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your

computer and disinfection of dangerous files. Kaspersky OnLine Scanner Pro runs directly in your web browser. Using the service, visitors can:

- Exclude archives and email databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for data stored 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 Mobile

Kaspersky® Anti-Virus Mobile provides antivirus protection for mobile devices running Symbian OS and Microsoft Windows Mobile. The program delivers comprehensive antivirus protection:

- **On-demand scan** of mobile device memory, memory cards, individual folders or a specific files. If an infected file is detected, it is moved to Quarantine folder or is deleted;
- **Real-time protection:** automatically scans all inbound or modified objects and files when attempts are made to access them;
- **Scheduled scans** of data stored in the mobile devices memory;
- **Protection from sms and mms spam.**

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 protection³ 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 Linux, and Samba file storage systems.
- *Email systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2004 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, and Linux, and Samba file storage systems;
- *Email systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition;

³ Depending on the type of distribution kit.

- *Hand-held computers* (PDAs), running Symbian OS, Microsoft 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 undesired email (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of email 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 email traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited email. The product is compatible with any email system and can be installed on either an existing email 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 email transmitted via SMTP. The application contains a number of additional tools for filtering email traffic by name and MIME type of attachments and a number of tools reducing the load on the email system and preventing hacker attacks. DNS Black List support provides protection against emails coming from servers entered in these lists as sources distributing unwanted email (spam).

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange performs anti-virus processing of incoming and outgoing email messages, messages stored at the server and letters in public folders.

It 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 email systems. This application installed between the corporate network and the Internet scans all components of email messages for the presence of viruses and other malware (Spyware, Adware, etc.) and centrally filters e-mail for spam. This solution also includes some additional email traffic filtration features (by name and MIME type of attachments) and a number of features that help reduce the load on the mail server and prevent hacker attacks.

Kaspersky Anti-Virus® for Proxy Servers

Kaspersky Anti-Virus® for Proxy Servers is an antivirus solution for protection web traffic routed through proxy servers via HTTP protocol. The application scans web traffic for viruses in real time, protects you from malware penetrating your system while web surfing, and scans files downloaded from the Internet.

Kaspersky Anti-Virus® for MIMESweeper for SMTP

Kaspersky Anti-Virus® for MIMESweeper for SMTP provides high-speed scanning of SMTP traffic on servers that use Clearswift MIMESweeper.

The program is a plug-in for Clearswift MIMESweeper for SMTP and scans for viruses and processes inbound and outbound e-mail traffic in real time.

B.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. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

| | |
|---------------------|--|
| Technical support | Please find the technical support information at http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html |
| General information | WWW: http://www.kaspersky.com http://www.viruslist.com Email: info@kaspersky.com |

APPENDIX C. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY ANTI-VIRUS (“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 ENTITY) CONSENT TO BE BOUND BY AND BECOME A 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 PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) 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 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 code with which you will be provided by Kaspersky Lab as part of the Kaspersky Anti-Virus 6.0.

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.

1.1 *Use.* The Software is licensed as a single product; it may not be used on more than one computer 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 computer 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 computer. 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 The Software protects computer against viruses whose signatures are contained in the threat signatures database which is available on Kaspersky Lab’s update servers.

1.1.3 If you sell the computer on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 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.

1.1.5 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 (other than as expressly permitted herein).

1.1.6 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.

1.1.7 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.8 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.

2. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of activation on:

- (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 enter activation code 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.

Support Services shall become available after Software activation. Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

(ii) 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.

(iii) 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.

(iv) "Support Services" means:

- (a) Hourly updates of the anti-virus database;
- (b) Free software updates, including version upgrades;
- (c) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;
- (d) Virus detection and disinfection updates in 24-hours period

- (v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your computer.

3. *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.

4. *Confidentiality.* You agree that the Software and the Documentation, including the specific design and structure of individual programs 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 activation code.

5. *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 your 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).

6. *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, Kaspersky Lab 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.

7. 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.

When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).