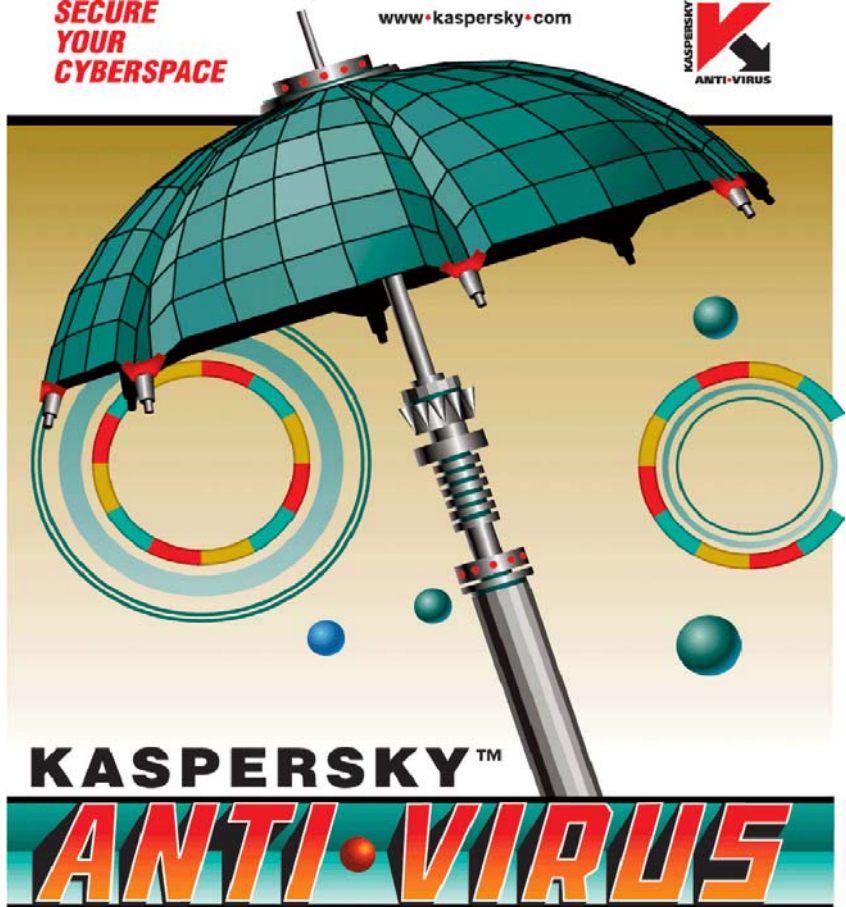


KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



Kaspersky Anti-Virus® 5.5 for Microsoft Exchange Server 2000/2003

Administrator's Guide

KASPERSKY ANTI-VIRUS® 5.5 FOR MICROSOFT
EXCHANGE SERVER 2000/2003

Administrator's Guide

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

Revision date: June, 2005

Table of Contents

CHAPTER 1. INTRODUCTION	6
1.1. Computer viruses and malicious software.....	6
1.2. The purpose and major functionality of Kaspersky Anti-Virus	8
1.3. What's new in version 5.5?	10
1.4. Software system requirements	11
1.5. Hardware system requirements.....	12
1.6. Distribution kit	13
1.7. Services provided for registered users	13
CHAPTER 2. OPERATION OF KASPERSKY ANTI-VIRUS.....	15
2.1. Security Server architecture.....	16
2.2. Deployment of anti-virus server protection	16
2.3. Anti-virus protection system maintenance.....	17
2.4. Application's operation on a cluster of servers	18
CHAPTER 3. INSTALLING, UPDATING AND REMOVING THE APPLICATION.....	20
3.1. Installing the application	20
3.1.1. First-time installation	21
3.1.2. Reinstalling the application.....	26
3.2. Upgrading to a new version	27
3.3. Removing the application.....	28
CHAPTER 4. STARTING USING THE APPLICATION.....	30
4.1. Starting the application	30
4.2. Application interface	30
4.2.1. Main application window	30
4.2.2. Shortcut menu	32
4.3. Creating the list of managed servers	33
4.4. Connecting the Management Console to the server	34
4.5. Minimum required configuration.....	35
4.6. Mail server protection without additional configuration.....	36
4.7. Verifying the application performance	38

4.7.1. Test “virus” EICAR and its modifications	38
4.7.2. Testing the correct operation of the application.....	39
CHAPTER 5. ANTI-VIRUS PROTECTION	41
5.1. Anti-virus protection levels.....	43
5.2. Enabling and disabling the anti-virus server protection. Selecting anti-virus protection level.	45
5.3. Scanning attachments.....	47
5.4. Actions to be performed on infected objects	51
5.5. Anti-virus protection efficiency.....	56
5.6. Background scan.....	58
CHAPTER 6. UPDATING THE ANTI-VIRUS DATABASE.....	61
6.1. Downloading updates from the internet.....	62
6.2. Downloading updates from a shared network folder	64
6.3. Automatic updates.....	66
6.4. Manual updating	67
CHAPTER 7. BACKUP COPYING	68
7.1. Viewing backup storage	69
7.2. Backup storage filter	70
7.3. Restoring objects from the backup storage.....	72
7.4. Sending objects for analysis	74
7.5. Deleting objects from the backup storage	75
7.6. Configuring the backup storage settings	75
CHAPTER 8. NOTIFICATIONS	78
8.1. Viewing and editing notification parameters	79
8.2. Creating a notification template.....	82
CHAPTER 9. PREVENTING VIRUS OUTBREAKS.....	86
9.1. Viewing and modifying virus outbreak notification settings.....	88
9.2. Creating a new virus outbreak counter.....	90
CHAPTER 10. REPORTS.....	95
10.1. Receiving reports.....	97
10.1.1. Viewing and modifying the report templates.....	98
10.1.2. Creating a report template.....	101
10.2. Viewing reports.....	104

CHAPTER 11. APPLICATION'S EVENTS LOGS	108
11.1. Configuring the diagnostics level	109
11.2. Configuring logs settings	111
CHAPTER 12. LICENSE KEYS	112
12.1. License information	114
12.2. License key details	116
12.3. License-related notifications	118
12.4. Installing the license key	119
12.5. Removing a license key	120
12.6. Unprotected storage areas	120
CHAPTER 13. FREQUENTLY ASKED QUESTIONS.....	123
APPENDIX A. TABLE OF SUBSTITUTION MACROS	126
APPENDIX B. GLOSSARY	128
APPENDIX C. KASPERSKY LAB.....	132
C.1. Other Kaspersky Lab Products	133
C.2. Contact Us.....	137
APPENDIX D. LICENSE AGREEMENT	138

CHAPTER 1. INTRODUCTION

The main source of viruses today is the global Internet. Most cases of the virus infection happen through the use of e-mail. The facts that almost every computer has e-mail client applications installed and that malicious programs are able to take a full advantage of software address book in order to find new victims are favorable factors for the distribution of malware. Without even suspecting it, the user of an infected computer is sending infected e-mail messages to his or her contacts, who, in turn, send new waves of infected messages and so on. It is not uncommon when infected files, due to someone's negligence, enter commercial mailing lists of large companies. In this case, the virus will affect not just five, but hundreds or even thousands recipients of such mailings who then will send infected files to dozens thousands of their contacts.

Apart from the threat of virus or malware infection, there is a problem of unsolicited e-mail messages and misuse of the internet resources. Not being a direct threat by itself, unsolicited e-mail messages (SPAM) cause the loss of working time and inflict serious financial losses.

Additionally, it is to be noted that the newest malicious programs use the so-called spamming technologies for efficient mass distribution and the methods of social psychology to make the user open the message, etc. Therefore, SPAM filtering is important not only for convenience, but also in order to protect your computer against some new types of viruses.

It is now acknowledged that for some companies information has become a more important asset than its physical property or cash. At the same time, in order to gain profit through the use of the information, it has to be available to the company's employees, clients and partners. This raises the issue of data security and, as its important element, the issue of protection of the corporate mail servers against the external threats, preventing virus outbreaks within the corporate networks and filtering out the unsolicited correspondence.

1.1. Computer viruses and malicious software

As the number of computer users grows and the exchange of information via the Internet and email increases in volume, there is an increased threat of computer virus infection and data corruption or capture by malicious computer programs or malware.

In order to be aware of potential threats to your computer, it is helpful to know what the types of malicious software ("malware") are and how they work. In general, malicious programs fall into one of the following three categories:

- **Worms** use network protection vulnerabilities for distribution. These programs were called "worms" because of their ability to tunnel from one computer to another, using networks, email and other channels. Due to this ability, worms can spread extremely fast.

Worms penetrate a computer, determine IP addresses of other computers, and send copies of themselves to these computers. Worms also utilize data contained in the address books of mail clients installed on the infected machine for sending infected messages. They can create work files on disks but may not utilize any resources of the infected computer except memory.

Penetration of a worm is a preliminary stage that is often followed by penetration of other malicious programs into the infected computer. For example, a worm may identify some vulnerabilities that Trojans will use later to penetrate the computer.

- **Viruses** infect computer programs by altering the way that infected programs work to gain control over the infected files when such files are run. This simple definition helps determine that the main action a virus performs is infecting computer programs. Viruses spread somewhat slower than worms.
- **Trojan horses** perform unauthorized actions on infected computers: for instance, they can erase information on hard drives, "freeze" the system, steal confidential information. In the strict sense, Trojan Horses are not viruses as they do not infect programs or data, and are unable to sneak independently into computers but are distributed by malicious users as "useful" software. Still the damage inflicted by Trojans may be far greater than from a regular virus attack.

Recently, worms have become the most widespread type of malware, followed by viruses and Trojans. Some malicious computer programs have characteristics of two or even all three of the above categories.

The following potentially dangerous types of malware have also become widespread:

Adware – code that, without the user's knowledge, is included into a program's code in order to display advertising messages. As a rule, adware is integrated into freeware programs. The advertising component is located in the interface. Adware programs are often used to gather users' personal information and send it to the developer, change browser's settings (browser's home page, search page, security levels, etc.) and create traffic that is not controlled by the user. All this may lead to the infringement of the security policy and further to direct financial losses.

Riskware – programs that are not supposed to perform any malicious functions, but contain security breaches and errors and therefore can be used by intruders as an auxiliary component of a malicious program. This type of software includes, for example remote administration programs, IRC client programs, FTP programs and various utilities used for ending or hiding running processes.

Spyware – software used to obtain unauthorized access to user's data, tracking actions performed on this computer, gathering information about the contents of the hard drive. Such programs help the intruder not only gather information, but also gain control over the user's computer. Spyware programs are often distributed along with freeware and installed on the user's computer without the user's knowledge. This type of software includes keyboard spies, password hacking programs and software used for gathering confidential information (for example credit card numbers).

Automatic dialers (*Pornware*) – programs that establish modem connection with various pay-per-visit internet (as a rule, pornographic) resources

Hacking tools – tools used by hackers to obtain access to the user's computer. This type of software includes various illegal vulnerability scanners, password hacking programs and other types of software used for hacking network resources or for obtaining unauthorized access to the system under attack.

Although malicious programs are distributed mainly via email and the Internet, a floppy disk or a CD can also be a source of infection. Therefore, the task of comprehensive protection from potential threats now extends far beyond simple regular scans for viruses, and includes the more complex task of real-time anti-virus protection.



Henceforth in the text of this User's Guide the term "virus" will be used to refer to viruses, Trojan Horses, worms and potentially dangerous programs and the term "dangerous objects" will be used to refer to objects infected with them. A particular type of malware will be mentioned only when it is required.

1.2. The purpose and major functionality of Kaspersky Anti-Virus

Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003 (hereinafter referred to as **Kaspersky Anti-Virus**) is designed to ensure the anti-virus protection of mail boxes and public folders located at Microsoft Exchange Server 2000/2003 (hereinafter referred to as **Microsoft Exchange Server**).

The major functionality of Kaspersky Anti-Virus includes:

- *scanning and analyzing incoming and outgoing e-mail messages* for the presence of malicious objects. This analysis covers all attributes and attachments of the e-mail message being scanned.
- *processing attributes and attachments of the e-mail message*. Depending on the settings selected, the application will disinfect or delete a malicious object or will add a warning message to such objects.
- *saving backup copies of the message's objects* before an attempt to disinfect or delete such object; copies are saved to a special storage for the consequent restoring which prevents the loss of data. Configurable filters allow to easily locate the original copies of objects.
- *notifying* the sender, the recipient and the system administrator about a message that contains a malicious object.
- *maintaining the events log and creating regular reports about the operation of the application and the status of the anti-virus protection*. The application allows to create reports using built-in templates with the required level of detail and at the required interval.
- *detecting virus outbreaks as they emerge and notifying about such events*. The application identifies attempts of mass-mailing infected messages both from the internet and from the computers within the corporate network.
- *configuring application settings* depending on the intensity and the nature of the traffic as well as the characteristics of the hardware installed (amount of RAM, speed, number of processors, etc.) both in the manual and in the automatic mode.
- *updating the anti-virus database* via internet both in the manual and in the automatic mode. The anti-virus database can be updated from the Kaspersky Lab's ftp and http servers.



Anti-virus scan and disinfection of infected objects are performed based on the records of the *anti-virus database* that contains description of all currently known viruses, methods used for the disinfection of objects infected with these viruses and description of potentially dangerous software.

As new viruses appear daily, it is very important to keep your anti-virus database up-to-date.

The anti-virus database at the Kaspersky Lab's servers is updated **on an hourly basis**. We recommend that you update the anti-virus database used by your application with the same frequency (see Chapter 6, page 61).

- *scanning old (previously scanned) messages for the presence of new viruses each time your anti-virus database is updated* or according to the

schedule. This task is performed as a background scan and *does not have any considerable effect on the performance* of the mail server.

- *creating the list of protected storage areas*, which offers additional flexibility in regards with license restrictions on the number of protected mail boxes.
- *managing license keys*.

Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server includes the following components:

- **Security server** that provides the anti-virus functionality and updating of the anti-virus database and includes administrative services for remote management, configuring and ensuring the integrity of the application and of the data stored.
- **Management Console** that provides the user interface for managing the administrative services of the application and allows to install the application, configure settings and manage the server component. The management module is implemented as the extension of the Microsoft Management Console (MMC).

1.3. What's new in version 5.5?

Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server has the following distinctions from the previous version:

- Completely revised intuitive graphical interface implemented according to the MMC (Microsoft Management Console) standards. Using the new interface, the administrator can start using the application without the need to configure any preliminary settings; this interface also offers a wide range of options for configuring the customized application management environment that can be adapted to the conditions of any particular corporate network to the maximum possible extent.
- The use of extended anti-virus database allows protecting your mail server not only against malicious software, but also against potentially dangerous software, such as adware, automatic dialing programs that connect the user's computer to commercial internet sites, hacking programs or joke programs.
- An option of selecting the anti-virus protection level has been implemented to enable the administrator to adjust the e-mail flow security level and the load on the server during the scan.
- Saving backup copies of objects before disinfection, deletion or renaming allows to restore objects or to send them to Kaspersky Lab for analysis. The possibility to create and use customized filters simplifies the search for information you need.

- The facility used for detecting virus outbreaks and for issuing notifications about such events allows to react to emergency situations in a timely fashion and to take timely measures aimed at the enhancement of the anti-virus protection of your mail server.
- A new feature has been added that allow user to scale the application based on the number of processors installed on the computer of the protected server. In order to enhance the efficiency of the application (increasing the number of objects that can be analyzed at the same time) several instances of the anti-virus kernel can be launched and run simultaneously.
- Memory object scanning capability has been expanded. Using scan settings configurations it is now possible to analyze up to 8 objects up to 1 MB each at the same time in RAM without using the disk subsystem, which results in a considerable increase in the application's efficiency.
- The logging capability has been drastically improved. Now this system allows setting up the degree of completeness of the data stored in the logs as well as the extent of detail of these data. Log viewing feature is implemented using the standard Microsoft Windows **Events viewing** application.
- This version includes a possibility to regularly create extended reports about the status of the anti-virus protection. Reports can be created either in the automatic mode or at the administrator's request. The reports maintaining system ensures fast, convenient and consistent method of accessing information using standard tools, as, for example, Microsoft Internet Explorer. The possibility to send reports by e-mail has been provided.
- A new feature has been added for notifying users about the detection of infected and suspicious objects and about virus outbreaks threats, using NET Send network tool.

1.4. Software system requirements

Requirements to protected Microsoft Exchange 2000 Server Enterprise Edition:

- Microsoft Windows Server 2000 with Service Pack 4 installed or higher or Microsoft Windows 2000 Advanced Server with Service Pack 4 installed or higher;
- Microsoft Exchange 2000 Server Enterprise Edition with Service Pack 2 installed or higher.

Requirements to protected Microsoft Exchange 2000 Server Standard Edition:

- Microsoft Windows Server 2000 with Service Pack 4 installed or higher or Microsoft Windows 2000 Advanced Server Service Pack 4 installed or higher;
- Microsoft Exchange 2000 Server Standard Edition.

Requirements to protected Microsoft Exchange 2003 Server Enterprise Edition:

- Microsoft Windows Server 2000 with Service Pack 4 installed or higher / Microsoft Windows 2000 Advanced Server with Service Pack 4 and higher installed or higher / Windows Server 2003 Standard Edition and higher / Windows Server 2003 Enterprise Edition and higher;
- Microsoft Exchange 2003 Enterprise Edition Server and higher.

Requirements to protected Microsoft Exchange Server 2003 Standard Edition:

- Microsoft Windows Server 2000 with Service Pack 4 installed or higher / Microsoft Windows 2000 Advanced Server with Service Pack 4 installed or higher / Microsoft Windows Server 2003 Standard Edition and higher / Microsoft Windows Server 2003 Enterprise Edition and higher;
- Microsoft Exchange 2003 Standard Edition Server and higher.

Requirements to the computer from which the application management will be performed:

- OS Microsoft Windows 2000 with Service Pack 4 installed or higher / Microsoft Windows XP / Microsoft Windows 2003 with MMC version 1.2 or higher.
- Active Directory Service Interfaces (ADSI) 2.5 or Active Directory Client Extensions (Microsoft Windows 2000 or higher automatically complies with this requirement).

1.5. Hardware system requirements

- Intel Pentium 300 MHz or higher;
- about 256 MB free RAM;
- about 20 MB free disk space for the application files (in addition to the size of the backup storage and other service folders).

1.6. Distribution kit

You can purchase Kaspersky Anti-Virus from our dealers (retail box) or online (for example, you may visit www.kaspersky.com and follow the **E-Store** link).

The retail box package includes:

- a sealed envelope with the installation CD containing the application files;
- User's Guide
- a license key written on a special disk;
- License Agreement



Before you open the envelope with the CD make sure that you have carefully read the license agreement..

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

License Agreement is a legal contract between you and Kaspersky Lab Ltd. which contains the terms and conditions on which you may use the anti-virus product which you have purchased.



Read the License Agreement carefully!

If you do not agree with the terms of this License Agreement, you can return the box with Kaspersky Anti-Virus to the dealer you purchased it from for a full refund provided that the envelope with the installation CD remained sealed.

By opening the envelope containing the installation CD or by installing the product on your computer you accept all terms and conditions of the License Agreement.

1.7. Services provided for registered users

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

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

- you will be receiving new versions of the purchased software product;

- support on issues related to the installation, configuration and use of the purchased software product. Services will be provided by phone or via email;
- information about new Kaspersky Lab products and about new viruses appearing worldwide (this service is provided to users who subscribe to the Kaspersky Lab's newsletter).



Support on issues related to the performance and the use of operating systems or other technologies is not provided.

CHAPTER 2. OPERATION OF KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus scans and, if it is possible, disinfects all incoming, outgoing e-mail messages as well as messages stored at the server. The application analyzes the body of the message and attached files of any format.

The scan for the viruses and the disinfection of infected objects are performed based on the records in the *anti-virus database* that is updated by Kaspersky Lab on a regular basis and contains description and the methods of disinfection of all currently known malicious programs, joke programs, potentially dangerous software and programs that are not potentially dangerous, but may be a part of the software used for development of such software.

The application performs a real-time scan of all e-mail messages arriving to the server. Before the message is scanned it cannot be viewed.

E-mail messages stored at the server and the content of all public folders are scanned each time the anti-virus database is updated or according to the schedule. The scan may identify new viruses that were not described in the anti-virus database at the time when previous scans were performed. This task is performed as a background scan and does not have any effect on the performance of the mail server. If the user requests a message that has not been scanned with the updated anti-virus database, such message will be scanned prior to the delivery to the user. Thus, the user will always receive e-mail messages that have been analyzed using the latest version of the anti-virus database, no matter when a particular message arrived to the server.

The application processes each object according to its current settings: it disinfects or deletes the infected object from the message, replacing it with the corresponding notification. The administrator may select a mode in which the application will deliver messages with infected objects to the user, although it will modify the object's name by adding information about the virus to it and change the object's extension.

Before processing an object, the application can save a copy of this object in a special backup storage for the consequent restoring or sending to Kaspersky Labs for analysis.

The program sends notifications about detected viruses to the administrator, to the recipient and to the sender of the infected message and enters corresponding records into the Windows application log and into the application's internal logs.

If the virus outbreaks detection tool is enabled, the application registers the virus activity level and sends notifications about a new virus outbreak threat or enters

corresponding records into the Windows application log and into the application's internal logs.

2.1. Security Server architecture

The server component of the application, Security Server, consists of the following subsystems:

- **E-mail Interceptor** – this component intercepts objects arriving to Microsoft Exchange Server and forwards them to the *anti-virus scan subsystem*. It is integrated into the Microsoft Exchange Server processes using VSAPI 2.0 and 2.5 technologies.
- **Anti-virus Scan Subsystem** performs anti-virus scan of objects. This component includes several processes with one anti-virus kernel per process. The anti-virus scan subsystem also includes a storage of temporary objects for scanning objects in RAM. The storage is located in working folder **Store** that is created in the installation folder and must be excluded from the scan scope of Kaspersky Anti-Virus for Windows File Servers or of other anti-virus applications.
- **The Internal Application Management and Integrity Control Module** is launched in a separate process and is an Microsoft Windows service. This service is launched automatically and does not depend on the state of Microsoft Exchange Server (started, stopped) which allows configuring the application even if Microsoft Exchange Server is stopped. For the correct operation of the application, the **Internal Application Management Module** must always be running; stopping this service manually is not recommended.

2.2. Deployment of anti-virus server protection



In order to create the mail servers anti-virus protection system, using Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server, perform the following:

1. Install the **Security Server** component on all protected Exchange servers. The installation shall be performed from the distribution kit individually for each server.
2. Install the **Management Console** on a computer within the corporate network. The Management Console provides a centralized access to all network resources from a single administrator's

workstation; therefore, it can be installed on one computer only. However, if several administrators are working jointly, the Management Console can be installed to each administrator's computer.



If the Management Console is not installed, the application will function within the default limitations and using the default settings(see para 4.6, page 36).

The anti-virus protection of the server will be enabled automatically when Microsoft Exchange Server is started and will be disabled when Microsoft Exchange Server is stopped.

3. Create the list of managed servers (see para 4.2.2, page 32)
4. Connect the Management Control to the servers (see para 4.4, page 34).
5. Configure the anti-virus protection system for each server:
 - Configure the anti-virus database updating settings (see Chapter 6, page 61).
 - Verify the correctness of the settings and of the Anti-Virus operation using a test "virus" EICAR (see para 4.7, page 38).
 - Configure the notification system that issues notifications about events registered during the application's operation (see Chapter 8, 78)
 - Configure the event logs and reports (see Chapter 10, page 95 and Chapter 11, page 108).
 - Configure the settings for detecting virus outbreaks and notification about such events. (Chapter 9, page 86).

2.3. Anti-virus protection system maintenance

Maintaining the server anti-virus protection in the up-to-date state involves:

- periodic updating of the anti-virus database;
- receiving and processing messages about detection of viruses and about threats of virus outbreaks;
- regular review of reports about the application operation and about the stage of the mail server anti-virus protection;
- processing and cleaning of the backup storage.

2.4. Application's operation on a cluster of servers

Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003 does not fully support the cluster technology; however, it will function correctly on a cluster of servers treating each node as a separate physical Exchange server.

A message arriving at a virtual Exchange server will be forwarded to one of the cluster's nodes. Streams of e-mail messages for each node may not intersect. Kaspersky Anti-Virus will process a message at the node to which this message had been forwarded by the virtual Exchange server.

The anti-virus scan results for each node of the cluster, namely,

- backup storage contents;
- information included into the reports;
- the group of events registered in the Windows logs and in the application's logs;
- values of virus outbreak counters

will be provided only for those messages that had been forwarded to this node of the cluster by the virtual Exchange server.



In order to create Microsoft Exchange Server anti-virus protection of the servers installed on the cluster:

1. Install the **Security Server** component to each node of the cluster. The installation shall be performed from the distribution kit individually for each server.

Specify a folder on a **local** disk of the server file system as the installation folder.



Shared disks should not be used for this purpose as when the Microsoft Exchange Server application is moved to a different node of the cluster, the shared disk will be moved along with the application.

2. Install the **Management Console** on a computer within the corporate network.
3. Create the list of managed servers by adding **all** cluster nodes as servers (see para 4.2.2, page 32).



When adding managed servers and configuring connection of Management Console to the Server, use the names of **physical** servers on which the Security Server is installed. The use of a **virtual** Exchange server name may cause an addressing error when the Microsoft Exchange Server is moved to a different node of the cluster.

4. Connect the Management Control to the servers (see para 4.4, page 34).
5. Configure the anti-virus protection system for each server using **identical** settings values taking into consideration the following:
 - As the backup storage folder, select a folder located on the physical server where the Security Server component is installed (see para 7.6, page 75).
 - As a folder to be used to store reports and logs, select folders located on the physical server where the Security Server component is installed (see para 10.1.1, page 98 and 11.2, page 111).
 - The list of unprotected storage areas on all servers must match (see para 12.6, page 120).

CHAPTER 3. INSTALLING, UPDATING AND REMOVING THE APPLICATION

Before the installation of Kaspersky Anti-Virus, make sure that the software and hardware of the computers used meet the installation requirements. The minimum requirements to the computers' configuration are provided in para 1.4, page 11.

3.1. Installing the application

The installation procedure is a standard one similar to that of most Windows applications. The setup wizard will offer you to install the application components of Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003, Security Server and Management Console, on the computer on which the setup wizard is run. This configuration is recommended at the initial stage of creating the Exchange servers anti-virus protection system. You can select either complete or custom installation of the application or repair an incorrect installation of Kaspersky Anti-Virus.



For installation of Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003 the local administrator's rights are required for the computer on which the installation is performed..

After the Management Console is installed, a shortcut icon for this component will appear in **Run/Programs/Kaspersky Anti-Virus Microsoft Exchange Server** menu in your computer.

The Security Server will be installed on your computer as a service with a set of attributes as follows:

- name – **Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003;**
- startup type – automatic;
- account – **Local system.**

The properties of the **Security Server** can be viewed and its operation can be monitored using standard Windows administration tools - **Computer Management/Services**. Information about the operation of the **Security Server** is registered and saved in the Windows applications log on the computer on which the Security Server is installed.

3.1.1. First-time installation

In order to install Kaspersky Anti-Virus into your computer run the `setup.exe` file on the installation CD included into the distribution package. The installation process will be facilitated by the setup wizard. Setup wizard will offer you to configure the installation parameters and start the installation. Following below is a detailed discussion of each step of the application installation.



The procedure used to install the application from the distribution kit downloaded from the internet is identical to the procedure used for application installation from the installation CD.

Step 1. Verifying the installed operating system version

Prior to the installation, a check will be performed to determine whether your operating system, mail application(s) and the Service Packs installed meet the software requirements for the installation of Kaspersky Anti-Virus. If these requirements are not met, a corresponding message will be displayed.

If Microsoft Exchange Server is not installed on your computer or if its version does not meet the software requirements, you can install only one application component – the Management Console. In this case, you have to install Microsoft Exchange Server that meets the software requirements and then reinstall Kaspersky Anti-Virus.

If any of the required Service Packs for the operating system or the mail system is not installed, perform the required updates and then reinstall Kaspersky Anti-Virus.

Step 2. Searching for other anti-virus software

Next step involves searching for other anti-virus products for Microsoft Exchange Server, including Kaspersky Lab's products, which may conflict with Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003.

If an incorrect registration of an anti-virus application for Microsoft Exchange Server is detected, the installation program will display a warning message with a suggestion to remove the registration detected.

In order proceed with the installation of Kaspersky Anti-Virus agree to remove the incorrect registration.

If other vendors' anti-virus software for Microsoft Exchange server is detected installed in your computer, a message will be displayed with a recommendation to remove such existing application before installing Kaspersky Anti-Virus.

Remove the existing program and then run the `setup.exe` file from the installation CD included into the distribution kit.

If an earlier version of Kaspersky Anti-Virus for Microsoft Exchange Server (for example version 4.5) is detected on your computer, a message will be displayed

requiring a removal of this program as it cannot be used with Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003.



We recommend that you save the current license key that you used with the previous version of the application (Kaspersky Anti-Virus for Microsoft Exchange Server 4.5) before you remove this version. You can use this key with Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003.

Remove the earlier version of the application and run the *setup.exe* file from the installation CD included into the distribution kit.

If Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003 is found installed on your computer, you will be offered to modify, restore or remove this copy of the application.

Step 3. Greeting and License Agreement

First steps of the installation process are standard and involve unpacking the required files from the distribution kit and copying them to the hard drive of your computer. After this, a greeting window and a window containing will the License Agreement will open. Read the text of the License Agreement and accept terms and conditions contained therein to proceed with the installation.

Step 4. Selecting the type of the installation

During the next step (see Figure 1), you will have to determine the type of the installation: complete or custom installation.

If the computer from which the installation is performed is a protected Exchange server and you plan to manage the application from this computer, select the complete installation option. In this case, both application components (the Security Server and the Management Console) will be installed. The application will be installed into the default folder (**Program files\Kaspersky Lab\Kaspersky Anti-Virus for Microsoft Exchange Server**).

If you wish to install only one component of the application (either the Security Server or the Management Console) or to change the default installation folder, use the custom type of the installation.

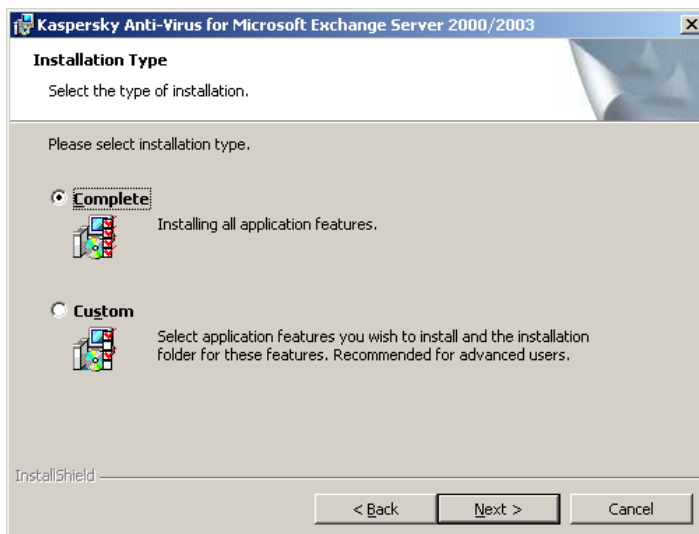


Figure 1. Selecting the type of the installation

Step 5. Selecting application components to be installed

If you use the custom installation, then during the next step (see Figure 2) you have to specify which application components must be installed on your computer. You can also change the default folder for the installation of these components.

If the computer, from which the installation is performed, is a protected Exchange server, select the **Security Server** component.

If this computer is the administrator's workstation and you plan to manage the anti-virus protection of the Exchange servers from this computer, select the **Management Console**.

Note that the setup wizard will display reference information about the selected component and the disk space required for its installation.

By default, the application components will be installed to the **Program files\Kaspersky Lab\Kaspersky Anti-Virus for Microsoft Exchange Server** folder. If this folder does not exist, it will be created automatically. You can change the default installation folder using the **Browse** button.

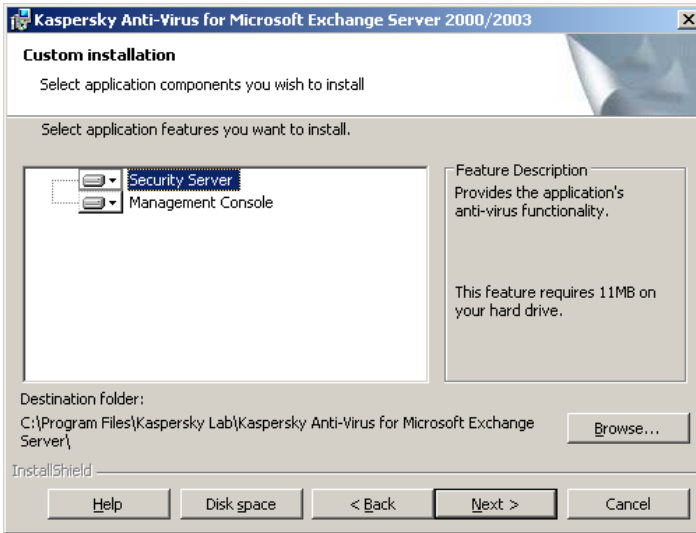


Figure 2. Selecting components for the installation

Step 6. Launching the installation process

After the settings are configured, launch the installation process. In order to do this, press the **Install** button. This will start the process of copying the application files to your computer.

After the copying is complete you will be offered to either automatically enable server anti-virus protection immediately after the wizard completes its work (see Figure 3) or do it manually later using the Anti-Virus Management Console (see section 5.2, page 45).

If the application performance at the level and with the parameters applied by default (see section 4.6, page 36) meets the requirements of your server, we recommend to accept the option of automatic anti-virus protection startup after completion of the installation wizard. Press the **Yes** button to proceed.

You should remember that by default all storage areas created on the server will be selected as protected storage areas. If the maximum number of protected mail boxes quoted by the license you have purchased is less than the number of storage areas created on the server, you must remove anti-virus protection from some of these areas before the protection is started (see section 12.6, page 120).

If you would like to configure the application settings before you start the anti-virus protection, disable the automatic anti-virus protection startup by pressing the **No** button.

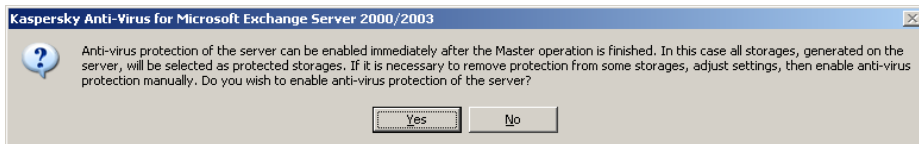


Figure 3. Prompt for enabling anti-virus protection

Step 7. Completing the setup

After the installation is complete, press the **Finish** button in the final window of the setup wizard.

If you are installing the Security Server component, you will be offered to install the license key (see Figure 4) for Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003. You can install the license key later, using the Management Console, but note that without the license key the anti-virus functionality of the application will not be available and you will only be able to start the Management Console.

Step 8. Installing the license key

During this step of the installation process, the license key for Microsoft Exchange Server is installed. The license key is your personal "key" that contains all service information required for the full-featured functionality of the application, namely:

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

In the **Installed license keys** window that will open (Figure 4) press the **Add** button. Specify the license key file (*.key) to be installed using the standard Windows Select file dialog box. As a result, the selected license key will be installed as the current license key for Kaspersky Anti-Virus.

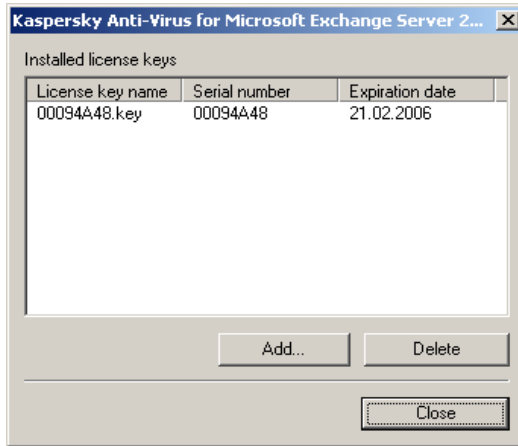


Figure 4. Installing the license key



If a copy of Kaspersky Anti-Virus 4.5 was installed on your computer and if the license key that was used with this version has not expired yet, you can use this key as the license key for Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003.

You can also install a backup license key that will be activated automatically upon the expiry of the current license key.

If, at the time of the installation, you still do not have the license key (for example you ordered it from Kaspersky Lab via internet but have not received it yet), you can install it later when you run the application for the first time using the Management Console. Note that without the license key you cannot start using Kaspersky Anti-Virus.

3.1.2. Reinstalling the application

Reinstallation of Kaspersky Anti-Virus is performed if the initial installation of the application was incorrect or during program operation the integrity of executable files was broken.



*In order to ensure the correct installation of the application, select the **Repair** option in the window that will open (see Figure 5)*

This will start reinstallation of Kaspersky Anti-Virus, which will use the same settings as the previous installation. For example, if the previous installation was a custom installation, then the reinstallation initiated by the **Repair** button will also be a custom type installation.

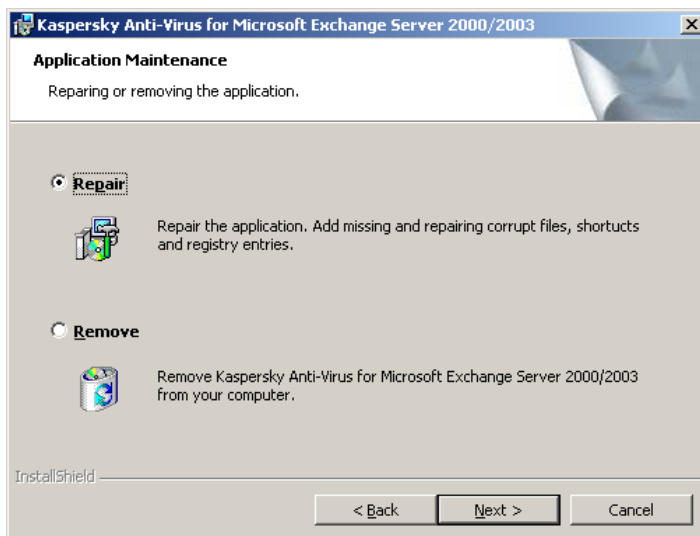


Figure 5. Selecting the application reinstatement mode

3.2. Upgrading to a new version

In order to upgrade version 4.x of Kaspersky Anti-Virus for Microsoft Exchange Server to version 5.5, remove the previous version and install a new one following the steps described in this Guide (details see para 3.1, page 20 and para 3.3, page 28).

RECOMMENDATIONS FOR MIGRATION FROM VERSION 4.5 TO 5.5

After installation, product version 5.5 starts working with a minimum set of parameters. Most of them are specified by default and correspond to optimal values recommended by Kaspersky Lab experts (see para 4.6, page 36).

Additional configuration should be performed manually. In order to make the system configuration identical to the settings used by version 4.5, you will have to enter the required changes. Please pay attention to the following during the procedure:

- Scanning of archives is disabled by default in version 5.5. You can enable it in the Scan attachments tab of the Anti-virus protection window (see para 5.3, page 47).
- Version 5.5 does not support unprotected user groups. Exclusion of objects from scanning is accomplished using unprotected storage. Storage protection can be configured in the Protected E-mail tab of the Anti-virus protection window (see para 12.6, page 120).

- Version 5.5 by default does not append notifications to event logs. You can configure addition of notifications to event logs in the Actions tab of the Properties: Notification name window that serves for setup of notification parameters (see para 8.1, page 79).
- While configuring notification parameters, specify the recipients' addresses only. You do not have to specify the SMTP server address because version 5.5 does not use SMTP for delivery of its notifications. You can configure notification parameters in the Actions tab of the Properties: Notification name window that serves for setup of notification parameters (see para 8.1, page 79).

3.3. Removing the application

You can remove Kaspersky Anti-Virus Microsoft Exchange Server 2000/2003 from your computer using standard Windows Add/Remove Programs tool or the application distribution kit. This will remove all installed Kaspersky Anti-Virus components (i.e. both the Security Server and the Management Console) from your computer.



In order to remove Kaspersky Anti-Virus for Microsoft Exchange Server 2000/2003 using the distribution kit:

1. Run the *setup.exe* file from the installation CD included into the distribution kit. The removal process will be facilitated by the application maintenance wizard. Follow its directions.
2. Select the application removal option in the window that will open (see Figure 6).
3. In the process of preparation for the application removal, a prompt will be displayed asking whether you wish to stop the Microsoft Exchange Information Store service (see Figure 7). Accept stopping this service.



After the procedure is completed, the setup program will return the service to its original status.

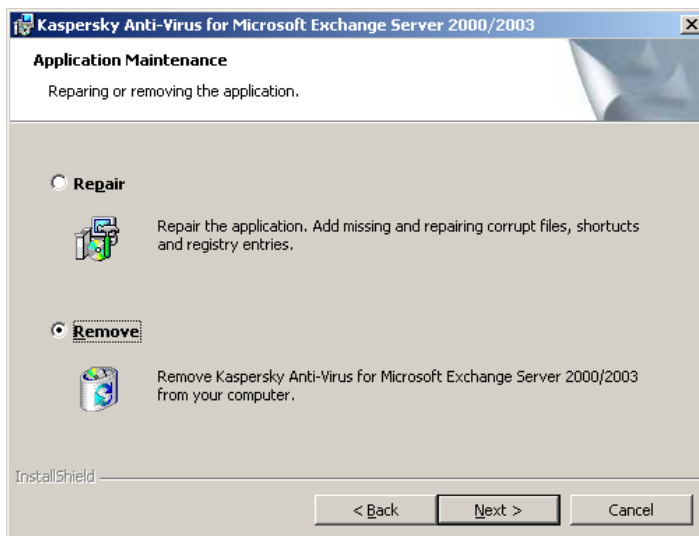


Figure 6. Selecting the application removal option

When removing the application using standard Windows **Add/Remove Programs** tool, a prompt asking whether you wish to stop the Microsoft Exchange Information Store service will also be displayed (see Figure 7). Accept stopping this service.



Figure 7. Stopping the Microsoft Exchange Information Store service

CHAPTER 4. STARTING USING THE APPLICATION

4.1. Starting the application

The server component of the application is started automatically at the operating system startup. If the anti-virus protection of the server is enabled (see para 5.1, page 43) it will be enabled immediately after the Microsoft Exchange Server is started.

The operation of Kaspersky Anti-Virus is controlled from the administrator's workstation – a computer on which the Management Console is installed.



In order to start the Management Console

select the **Management Console** item in the programs group **Kaspersky Anti-Virus for Microsoft Exchange Server** from the standard **Start / Programs** Windows menu. This programs group is created only on the administrator's workstations when the Management Console is installed.

4.2. Application interface

Kaspersky Anti-Virus user interface is provided by the Management Console component. The Management Console is a dedicated isolated facility integrated into MMC, therefore the application interface is a standard MMC interface.

4.2.1. Main application window

The main application window (see Figure 8) contains a menu, a toolbar, a view pane and a results pane. The menu provides the files and windows management functions as well as the access to the help system. The set of buttons on the toolbar ensures the direct access to some frequently accessed items of the main menu. The display pane presents the **Microsoft Exchange Server** namespace in the form of the console tree, the results pane displays the list of elements presented in the tree form.

The **Microsoft Exchange Server** namespace may contain several nodes with the names of the servers managed via the console. The namespace does not

contain any elements immediately after the installation of the Management Console.

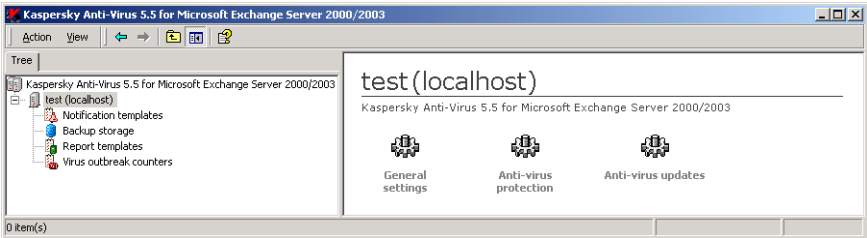


Figure 8. Main application window

After a new server is added, it is displayed in the console tree as a node **<Server Name>**. The settings configuration and controlling Kaspersky Anti-Virus application is performed using hyperlinks in the results pane.

- [General settings](#) – used for viewing general settings of Kaspersky Anti-Virus operation, license details and information about installed license keys, renewing the license and the configuring the application operation diagnostics settings.
- [Anti-virus protection](#) – used for viewing and configuring the managed server's anti-virus protection settings
- [Anti-virus database updates](#)– used to configure settings for downloading the anti-virus database updates, manual updates and setting up an automatic update schedule.

If the connection to the server was established, the **<Server name>** node will include nested folders; each of these folders is used for managing a particular function of the application.

- **Notification templates** – for configuring notifications about detection of infected or suspicious objects during an anti-virus scan.
- **Backup storage** – for working with the backup storage where backup copies of objects are stored; includes the list of objects stored in the backup storage.
- **Report templates** – for managing reports; contains a list of report templates used to create reports about the program operation and the status of the server anti-virus protection.
- **Virus outbreak counters** – for configuring the criteria for identifying virus outbreaks and settings used in notification about detected outbreaks.

4.2.2. Shortcut menu

Each category of objects in the console tree has its own shortcut menu. In addition to standard MMC commands, this shortcut menu contains commands used for handling a particular object. The list of objects and the corresponding set of commands accessible via the context menu are provided in the table below.

Object	Command	Purpose
Microsoft Exchange servers	Add a server	Add a new Exchange server with the Security server installed to be managed via the console.
<Server name>	Disconnect from the server	Disconnect an Exchange server with the Security server installed from the Management Console.
	Connect to the server	Connect an Exchange server with the Security server installed to the Management Console
	Remove the server from the console tree	Remove an Exchange server from the list of servers that have their Security servers managed via the Management Console.
Notification templates	New notification template	Create and configure a new notification template about infected and suspicious objects detected as a result of an anti-virus scan.
Backup storage	New filter	Create and configure a new filter used to search for objects located in the backup storage.
Report templates	New report template	Create a new report template.
Virus outbreak counters	New counter	Create and configure a new criterion to be used for identifying a virus outbreak and settings to be used for notification about such outbreak.

Additional shortcut menu commands are also provided for report templates and for the backup storage. Using the **Create a report** command you can create a report based on the selected template. The **Get file** command allows to obtain the original copy of the object that had been saved before this object was

processed by the anti-virus. **Send for analysis** – send an object from the Backup storage to Kaspersky Lab for analysis.

4.3. Creating the list of managed servers

In order to be able to control Kaspersky Anti-Virus via the console, the Exchange server, on which the Security Server component is installed, must be added to the list of managed servers. You can add to this list either a local computer or any Exchange server within the network. Adding a server may be accompanied by establishing a connection between the Management Console and Kaspersky Anti-Virus.



In order to add a server to the list of managed servers,

1. Select a **Microsoft Exchange Server** node in the console tree, open the shortcut menu and select the **Add a server** command or use the analogous item from the **Action** menu. This will open a **Adding a server** window (see Figure 9)
2. Specify a computer with the Security Server component installed. If the server component is installed on the same computer as the Management Console, select **Local computer**. In order to add an Exchange server from the computers installed in the network, select **Remote computer** and specify the name computer's name in the entry field. You can enter the name manually (select IP address, full domain name (FQDN in the following format **<Computer name>.<DNS-domain name>**), NetBIOS name (the computer's name in the Microsoft Windows network) or select the computer using the **Browse** button.



When the application is connecting the Management Console to the Security Server, the program will use this name to establish connection with the computer.

The connection is established using DCOM protocol.

In order to establish connection between the Management Console and Kaspersky Anti-Virus when adding the server, check the **Connect now** box (details see para 4.4, page 34).



The server you select must have the Security Server component installed.

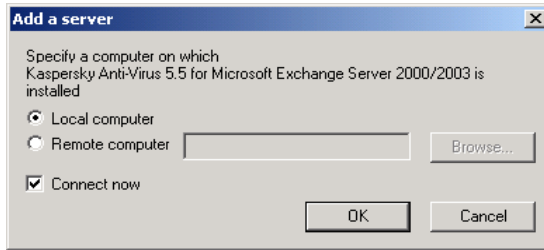




Figure 9. The **Add a server** dialog box

As a result, the server that you selected will be displayed as a **<Server name>** node in the console tree. The local computer will be displayed as the **<Server name>(localhost)**. If the connection with the server was successfully established, the  icon will appear next to it and the node structure will include nested folders: **Notifications**, **Backup Storage**, **Reports** and **Virus Outbreaks**. If the connection have not been established or could not be established or the servers could not be installed, the server will be flagged with the  icon. You can connect to such server only manually (see para 4.4, page 34).



In order to remove a server from the list of managed servers,

select the node that corresponds to the server you wish to remove in the console tree, open the shortcut menu and select the **Delete server from the console tree** command or use the corresponding item in the **Action** menu.

As a result, the selected node will be removed from the console tree.


4.4. Connecting the Management Console to the server

In order to be able to configure and manage Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server using the Management Console, you have to connect to the Security Server component installed on the server. The application will then receive information from the server and display it as the console tree.



In order to connect to the Security Server:

select the node that corresponds to the server you wish to remove in the console tree, open the shortcut menu and select the **Remove server** command or use the corresponding item in the **Action** menu.

If the connection with the server was successfully established, the settings of this server will be displayed in the main application window: the node will be flagged with the  icon and the node structure will include folders **Notifications**, **Backup storage**, **Reports** and **Virus Outbreaks**.

If the connection could not be established, the application will display a warning (see Figure 10) with the indication of the problem and a suggestion to connect next time the Management Console is started. Select the required option.



In order to connect to the Security Server, the user must have the local administrator's right on the computer to which the connection is attempted.

The rights verification is performed based on the standard Windows network user authentication process.

One Security Server can have several Management Consoles connected to it. In this case, with the operation using several consoles communicating with the server, it is necessary to update information on each console. In order to do this, use the **Update** command available via the shortcut menu or the similar command in the **Action** menu.



Figure 10. Console to Server connection error

4.5. Minimum required configuration

After the installation, Kaspersky Anti-Virus will start working with the minimum set of settings, most of which are default optimum settings recommended by the Kaspersky Lab's experts. If necessary, depending on the network properties and the characteristics of the computer on which Microsoft Exchange Server is installed, you can make all required changes and additions.



If you connect to the internet using a proxy server, you will have to configure your connection settings to receive updates.

In order to ensure full functionality of the mail server protection, it is necessary to configure settings used to notify the administrator and other users about the detection of infected and suspicious objects and about virus outbreaks threats.

The application settings are configured from the administrator's workstation – a computer on which the Management Console is installed. This operation can be performed irrespective of whether the Microsoft Exchange server application is running on the server.

4.6. Mail server protection without additional configuration

Anti-virus protection of the Exchange server starts operating immediately after the Security Server component is installed. The default operation mode of the application is as follows:

- The Anti-Virus will scan objects for the presence of currently known malicious software (with the standard anti-virus protection level applied)
- Anti-virus protection will be provided for all public folders, all storage areas created at the Exchange server and all users registered with the particular mail server.
- All new e-mail messages arriving to the Exchange server and having the following parameters will be scanned for viruses:
 - the body of the message and attached objects of any format will be scanned, except archives and containers with the level of nesting above 32;
 - the maximum time for scanning 1 object is 180 seconds;
 - when an infected object is detected, the application saves a copy of this object (attachment or the body of the message) in the backup storage, then attempts to disinfect the object and, if disinfection is impossible, the application deletes the object and replaces it with a text file containing a notification in the following format:

```
Malicious object %VIRUS_NAME% has been
detected. File (%OBJECT_NAME%) was deleted by
Kaspersky Anti-Virus.
```

If an object that cannot be disinfected is detected in the body of the message, the body of the message will be replaced with a similar text notification.

- when a suspicious object is detected, the application will save a copy of this object (attachment or the body of the message) in the backup storage.

Suspicious objects detected in message body are replaced with a notification of the following format:

Virus (possibly %VIRUS_NAME%). File (%OBJECT_NAME%) was deleted by Kaspersky AV

If a suspicious object is detected in the attached file, the application will change filename and extension of attached objects. Renamed objects will have *txt* extension.

- when a protected or corrupt object is detected, the application will save a copy of this object (file or the body of the message) in the backup storage.

Objects detected in message body are replaced with a notification of the following format:

The attached file %OBJECT_NAME% was deleted by Kaspersky AV. File was password-protected or corrupted

If a protected or corrupt object is detected in the attached file, the application will change filename and extension of attached objects. Renamed files will have *txt* extension.

- Messages stored on the server as well as the content of public folders are not scanned.
- Mail traffic routed by the Exchange server will not be scanned.
- The anti-virus database is updated hourly via internet from the Kaspersky Lab's HTTP and FTP servers.



If you connect to the Internet using proxy-server, you should configure connection settings for successful updates download.


- The administrator will not be notified about infected and suspicious objects detected.
- The detection of virus outbreaks will be recorded: detection of infected objects will be recorded five times a day without issuing notifications to the administrator.

Reports on the status of the anti-virus protection system are created on the first day of each month and covers last 30 days.

4.7. Verifying the application performance

After Kaspersky Anti-Virus is installed and configured, we recommend verifying the correctness of its settings and operation using a test "virus" and its modifications.

4.7.1. Test "virus" EICAR and its modifications

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

The test "virus" IS NOT A VIRUS because it does not contain code that can harm your computer. However, most anti-virus products manufacturers identify this file as a virus.



Never use real viruses for testing the operation of an anti-virus product!

You can download this test "virus" from the official website of the **EICAR** organization at http://www.eicar.org/anti_virus_test_file.htm. If you have no Internet connection, you can create your own test "virus". To create a test "virus," type the following string in any text editor and save the file as **eicar.com**:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

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

To test the response of Kaspersky Anti-Virus when other types of objects are detected, modify the content of this standard test "virus" by adding one of the prefixes listed in Table below.



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

Prefix	Object type
No prefix, standard test "virus"	Infected – An error occurs during an attempt to disinfect the object; apply action set for objects that cannot be disinfected.
CORR-	Corrupted
SUSP-	Suspicious (unknown virus code)
WARN-	Warning (modified code of a known virus)
ERRO-	Not analyzed due to an error.
CURE-	Infected The object will be disinfected; the text of the "virus" body will be replaced with the word "DISINFECTED"
DELE-	Infected Apply action set for objects that cannot be disinfected.

The first table column lists prefixes to be added at the beginning of the string of the standard test "virus" (for example, DELE-X5O!P%@AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*).

After adding a prefix to the test "virus" save it, for example, to a file under the name *ecar_dele.com* (assign names to all the modified "viruses" in the same manner).

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

4.7.2. Testing the correct operation of the application

After the application is installed, we recommend that you test how Kaspersky Anti-Virus handles incoming and outgoing e-mail messages including both the body of the message and the attachments.



In order to test detection of viruses in the body of the message,

1. Create a message in the **Plain text** format using the mail client installed on your computer.



If the message that contains a test "virus" was created in the RTF or HTML format, it will not be scanned.

2. Copy the text of the standard or the modified test "virus" to the beginning of the message body.
3. Send this message to the administrator's address.
4. Read the message received at the specified address.

CHAPTER 5. ANTI-VIRUS PROTECTION

The main task of Kaspersky Anti-Virus is scanning mail traffic and disinfection of mail messages using the information contained in the current (latest) version of the anti-virus database.

Depending on the anti-virus protection level selected by the administrator (see section 5.1, page 43), the application allows detection of:

- malicious objects;
- potentially dangerous objects;
- objects that are not potentially dangerous, but may be a part of software used for development of such objects;

All mail messages arriving to the Exchange server are scanned in the real-time mode. The processing is provided both for the incoming and outgoing traffic. The traffic routed by the Exchange server can also be scanned. In order to decrease the load on the server, you can disable the scan of the transit mail traffic (details see para 5.3, page 47).

When the traffic scan mode is enabled, the application remains loaded in the computer's RAM and the **E-mail Interceptor** analyzes the mail traffic received from the Exchange server and transfers it to the **Anti-Virus Scan Subsystem**. The **Anti-Virus Scan Subsystem** processes the e-mail messages based on the settings as follows:

- scans and analyzes the object using the anti-virus database;
- if an e-mail message or its part is infected, the application processes the detected object in accordance with the selected settings (details see para 5.4, page 51);
- before the processing, a copy of the object can be saved in the backup storage.

If the anti-virus server protection is enabled (details see para 5.1, page 43), then starting and stopping of the traffic scan will be performed simultaneously with the starting and stopping of the Microsoft Exchange Server.



When using Microsoft Exchange Server 2000, the incoming mail will be scanned irrespective of the mail client application and the mail protocol used. Outgoing messages will be scanned only if an Microsoft Exchange Server compatible client (as for example, Microsoft Outlook) and MAPI protocol are used for sending e-mail messages. In all other cases outgoing messages will not be scanned as they are not transferred to the backup storage on the protected server.



Kaspersky Anti-Virus does not scan messages created by protected users in the **Public folders** of unprotected Exchange servers.

E-mail messages stored on the server and the content of public folders are also rescanned on a regular basis using the latest version of the anti-virus database. The scan is performed in the background mode and can be launched either automatically each time the anti-virus database is updated, or according to the schedule, or manually (details see para 5.6, page 58).



If the background scan mode is enabled for the application used on a servers cluster, the background scan can be started when the Microsoft Exchange Server is moved from one cluster node to another.

If the background scan mode is disabled, then the messages stored on the server will be scanned only when the user requests a message, immediately before the delivery.



Operation of the application in the background scan mode may slow down the operation of Microsoft Exchange Server, therefore we do not recommend using this type of protection frequently.

When the background scan is enabled, the **Internal Application Management Module**, based on the settings, will receive from the Exchange server all e-mail messages located in the public folders and protected storage areas. If a message has not been analyzed using the latest anti-virus database, the application will send it to the **Anti-Virus Scan Subsystem** for processing. Objects processing in the background mode is performed the same way as in the traffic scan mode.

The application will analyze the body of the message and attached files of any format.

It is to be noted that Kaspersky Anti-Virus differentiates between simple objects (an executable file, a message with a simple attachment) from containers (consisting of several objects, for example, an archive or a message with any message attached to it).



Please note that the application does not scan multiple volume archives for viruses and such archives can be scanned after they are saved to disk, with, for example, Kaspersky Anti-Virus for Windows File Servers installed on this computer.

If necessary, you can define the list of objects that should not be scanned for viruses. The following types of objects can be excluded from the scan scope: all containers above the specified nesting level, file specified by a mask or files specified by a type (details see para 5.3, page 47).

Kaspersky Anti-Virus supports scanning several objects at the same time. The number of objects that can be processed at the same time depends on the

number of started instances of the anti-virus kernel running simultaneously. The mode of scanning objects in RAM allows scanning objects without saving them to a temporary folder on the hard drive. Depending on the scan settings, the program can simultaneously analyze up to 8 objects up to 1 MB each in the computer's RAM without using the disk subsystem (details see para 5.5, page 56).



Files over 1 MB will be saved to a working folder **Store** for processing. The **Store** folder is located in the installation folder of the application. The **Store** folder and the temporary file storage – folder **TMP** must be excluded from the scan scope of Kaspersky Anti-Virus 5.0 for Windows File Servers or of other anti-virus applications.

5.1. Anti-virus protection levels

Kaspersky Anti-Virus allows detecting and preventing the penetration of the following types of objects through the mail server:

- a. All currently known malicious programs.
- b. Programs that do not contain malicious code as it is commonly understood, but may impose a moral threat, inflict financial damage or facilitate abduction of confidential information. This software category includes:
 - adware;
 - various harmless utilities that can be used by malicious software and intruders;
 - automatic dialing programs that connect the user's computer to commercial internet sites;
 - automatic dialing programs that connect the user's computer to porn websites;
 - automatic porn files downloading programs;
 - keyboard spies;
 - password hacking programs;
 - backdoor programs,
- c. Joke programs and programs with "bizarre" content or form programs that affect the system in a way that cannot be qualified as beneficial. This type of software include:
 - programs that cause unexpected video or sound effects;
 - programs that cause problems in the system operation;

- virus simulators.
- d. Programs that do not contain malicious code and do not inflict any damage to the user, but can be a part of the environment used for development of malicious software. This software category includes:
 - licensed software hacking programs, key generators, credit card numbers generators;
 - Java classes;
 - programs that gather information about the system security (anti-virus software installed, firewalls, etc.)
 - network utilities (scanners, etc.)

Apart from the programs listed above, each of the above categories may include legal software that may work in a way that can be viewed by the Anti-Virus as a behavior characteristic of malicious or potentially dangerous software. An example of such software are backdoor and remote surveillance software.

If you transfer software via your mail server, the type of program you are transferring should be excluded from the list of objects scanned (see section 5.3, page 47).

Categories of objects detected by the Anti-Virus in the mail flow of the protected server are determined by the anti-virus protection level selected. The application provides for the following protection levels:

- **Standard anti-virus protection level:** protection against all currently known malicious programs. This level is applied by default.
- **Extended anti-virus protection level:** protection against all currently known malicious and potentially dangerous programs included under 'a' in the list above.
- **Superfluous anti-virus protection level:** protection against all currently known malicious programs and potentially dangerous software included under c and d in the list above.

5.2. Enabling and disabling the anti-virus server protection.

Selecting anti-virus protection level.

If the anti-virus server protection is enabled, then the anti-virus scan of the e-mail traffic will be started when the Microsoft Exchange Server is started or stopped. If the anti-virus protection settings provide for the background scanning of storage areas, then it will be started either when the anti-virus database is updated or according to the schedule (details see para 5.6, page 58).

If the anti-virus server protection is disabled, then neither the anti-virus traffic scan nor the background storage scan will be performed.



It is to be noted that disabling the anti-virus server protection considerably increases the risk of malware penetration via the e-mail system. We do not recommend disabling the anti-virus protection for long periods of time.



In order to enable or disable the anti-virus protection or change anti-virus protection level.

1. Select the node corresponding to the server you need in the console tree and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **General** tab in the **Anti-virus protection** (see Figure 11) window that will open.

Select the one of the following options in the Anti-virus protection group of fields:

- **Disabled** - in order to disable anti-virus protection of the mail system.
- **Standard anti-virus protection, Extended anti-virus protection or Superfluous anti-virus protection** - in order to enable anti-virus protection of the mail system using the corresponding level.



The use of the extended or the superfluous anti-virus protection level may affect the speed of the Anti-Virus operation. Besides, some programs may be referred to potentially dangerous programs when transferred by mail.

3. In order to apply the changes, press the **Apply** or the **OK** button. The anti-virus protection will then be enabled (or disabled) in several minutes.

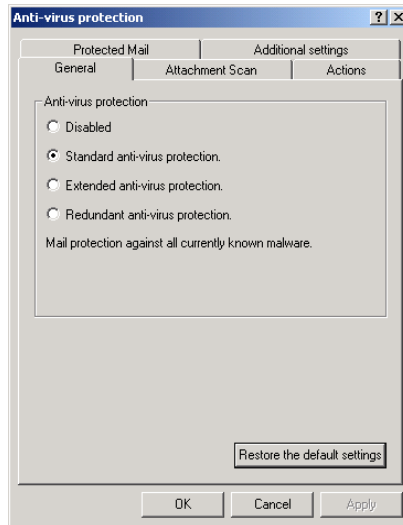


Figure 11. Enabling the anti-virus protection



We do not recommend disabling the anti-virus protection by disabling the Kaspersky Anti-Virus 5.5 for MS Exchange Server 2000/2003 service manually using the **Computer Management / Services** utility.



If you still need to disable Kaspersky Anti-Virus 5.5 for MS Exchange Server 2000/2003 service manually, do the following:

1. Disable anti-virus mail protection using the **Management Console**.
2. Restart the Exchange Information Store.
3. Specify the **Disabled** startup type for Kaspersky Anti-Virus 5.5 for MS Exchange Server 2000/2003.



In order to start the Anti-Virus after the automatic startup of the Kaspersky Anti-Virus 5.5 for MS Exchange Server 2000/2003 service had been disabled, do the following:

1. Specify the **Auto** startup type for Kaspersky Anti-Virus 5.5 for MS Exchange Server 2000/2003.
2. Restart the Exchange Information Store.

3. Enable the anti-virus mail protection using the **Management Console**.

5.3. Scanning attachments

In order to decrease the load on the server when the anti-virus scan is performed, you can limit the list of the objects to be scanned and put a restriction on the time for scanning one object. These scan restrictions will be used both for scanning the traffic and for the background storage scan.



It is to be noted that the body of the message will always be scanned as the restrictions apply only to the attachments.

In order to reduce the load on the server in the traffic protection mode it is recommended not to scan e-mail messages routed by the server.



In order to define objects that will not be scanned,

1. Select the node corresponding to the server you need in the console tree and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **Attachment Scan** tab in the **Anti-virus protection** (see Figure 12) window that will open.
3. In the **Exclude from the scan scope** group, specify objects that you wish to exclude from the anti-virus scan scope.
4. In order to restrict the time for processing one object check the **Stop scan if it takes longer than {NN} sec** box and specify the scan time in seconds.
5. After you are done with this setting, press the **Apply** or the **OK** button to apply the changes.

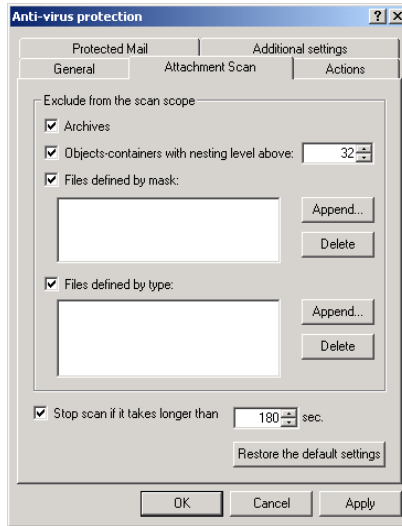


Figure 12. Configuring restrictions for the attachment scan

Since the scanning of archives and containers requires considerable time and server resources, you can decide yourself whether it is necessary to analyze these object.



In order to exclude archives from the scan scope:

in the **Exclude from the scan scope** group of boxes, check the **Archives** box.



In order to exclude containers from the scan scope:

in the **Exclude from the scan scope** group check the **Objects - containers with nesting level above** and specify the level. The application will scan all nested objects within the container including the specified level.

As the archives are a type of containers, the restrictions to scanning containers apply to archives as well.



If you impose a restriction on the scanning of containers, the same nesting level restrictions will be applied to the archives (if archives have not been explicitly excluded from the scan).

Exclusion of archives from the scan scope do not affect settings used to scan other types of containers.

Some objects cannot be infected. In order to decrease the load on the server when performing anti-virus processing of e-mail messages, we recommend to determine the types and/or the names of such files and filter them out when scanning the mail. In order to do this, use the exclusion settings by file masks and by the file types.



In order to exclude the objects from the scan scope using masks,

1. Check the **Files defined by mask** box in the **Exclude from the scan scope** group of boxes.
2. Create the list of exclusions using the **Append...** and the **Delete** buttons.

Enter a new mask in the **Adding a mask** (see Figure 13) window that will open.

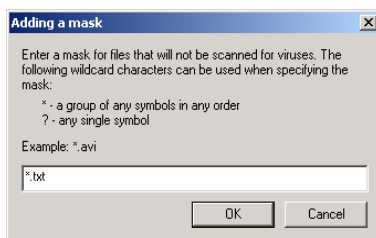


Figure 13. Adding a mask for files to be excluded from the scan scope

Examples of legal exclusions masks:

- ***.txt** – all files with mask ***.txt**
 - ***.tx?** – all files with mask ***.tx?**
 - **test** – all files with filename **test**
3. In order to apply the changes, press the **Apply** or the **OK** button.



In order to exclude objects from the scan scope by type,

1. Check the **Files defined by type** box in the **Exclude from the scan scope** group.
2. Create the list of objects types to be excluded from the scan scope using the **Append...** and the **Delete** buttons.

Add the type in the **Adding a type** dialog box (see Figure 14) by selecting the required type from the drop-down list:

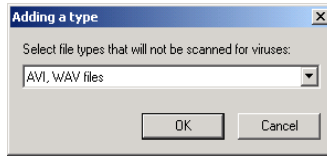


Figure 14. Selecting a type of files to be excluded from the scan scope

3. In order to apply the changes, press the **Apply** or the **OK** button.



In order to exclude mail sent to other servers from the scan scope,

1. Select the node corresponding to the server you need in the console tree and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **Protected mail** (see Figure 15) tab in the **Anti-virus protection** window that will open.
3. Check the **Do not scan routed mail** box **Routed mail (only for Microsoft Exchange Server 2003)** in the **Routed mail** group of boxes (checked by default)

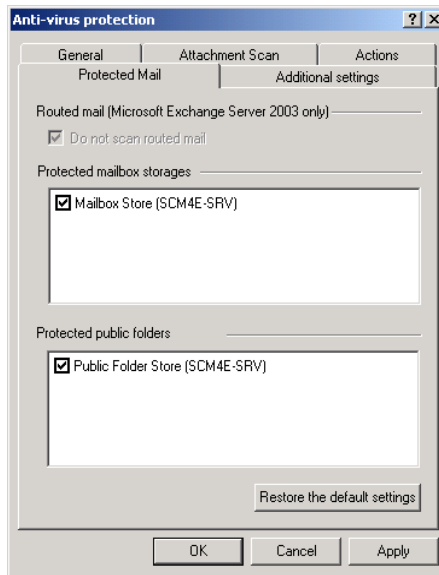


Figure 15. Excluding transit traffic from the scan scope

5.4. Actions to be performed on infected objects

As a result of an anti-virus scan each object can be assigned a status as listed below:

- **Not infected** – object does not contain viruses.
- **Infected** – object contains at least one of the known viruses.
- **Suspicious** – object's code is similar to the code of a known or unknown virus.
- **Protected** – object is password-protected.
- **Corrupted** – object is corrupted.

Which actions will be applied to an object depend on the object's status.

The most important major function of the application is the *disinfection* of **infected** objects. Disinfection is performed based on the information contained in the anti-virus database. According to the results of the attempted disinfection, an object can be assigned a status as listed below:

- **Disinfected** – object successfully disinfected.
- **Non-disinfectable** – object disinfection failed.

A special processing procedure can be used for **non-disinfectable** objects.



Infected objects found in the message body are processed using the action that is assigned to objects that could not be disinfected.

The following actions can be applied to objects with one of the following statuses: **infected, non-disinfectable, suspicious, protected and corrupted**.

- *Pass* – pass the object to the recipient with no changes.
- *Replace message body with text and rename attached objects* – change the infected message body with text created using the corresponding replacement template and change name and the extension of the infected attached objects. Such renamed objects will have *.txt* extension.



Names of the attached objects only will be changed, no changes will be made in the body of the message if the virus is detected.

- *Replace infected objects with text* – delete the detected object and replace it with text (message body) or a *txt* file (attachments) created based on the replacement template.

- *Delete the entire message* – delete the infected message along with all attachments (Microsoft Exchange Server 2003).



If the infected attachments are disinfected, replaced with text or renamed, a separate copy of a message for each recipient is saved in the Exchange server database. In order to reduce the size of this database we recommend that you defragment it periodically.

Before the processing, a copy of the object can be saved in the backup storage so that later it can later be restored or sent to Kaspersky Lab for analysis (see Chapter 7, page 68).

The application can send notification about the object detected to the administrator or to other users or register such event in the Windows events log (see Chapter 8, page 78 and Chapter 11, page 108).

By default, the application attempts to disinfect **infected** objects detected and if the disinfection is not possible, the application will replace the object with a txt file. To objects with a different status, the **Replace with text** action will be assigned.



If an object attached to the message was processed (disinfected, deleted, replaced) with Kaspersky Anti-Virus, then before the message is closed, your e-mail client application (for example, Microsoft Outlook) will offer you to save changes although the user has made no changes. You must save the message.



In order to define the order of processing of objects detected during an anti-virus scan,

1. Select the node corresponding to the server you need in the console tree and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **Actions** tab in the **Anti-virus protection** window (see Figure 16) that will open.

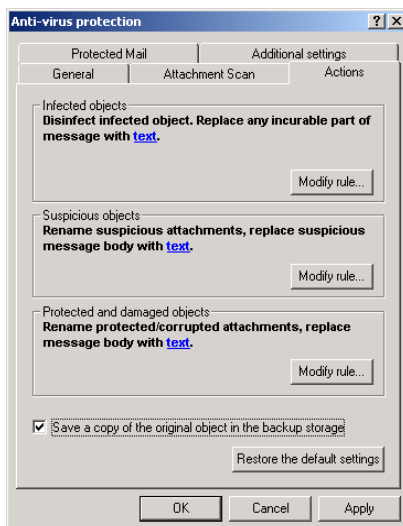


Figure 16. Configuring actions to be applied to infected objects

The tab displays the order used for processing objects with the followings statuses (each status individually): **infected**, **suspicious** and **protected/corrupted**.

3. Determine the order of the object processing of for each status individually. In order to do this, press the **Modify rule...** button in the corresponding section. As a result the Master is started. Follow its instructions.
4. In the window that will open (see Figure 17). select actions from the list.

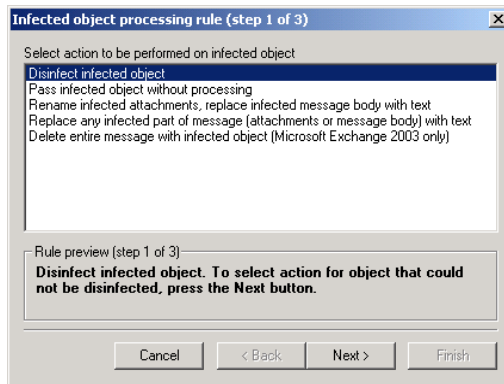


Figure 17. Creating the replacement template

Depending on the status of the object for which configuration is performed, the list may contain different values. A detailed description of the option selected in the table is provided in the bottom part of the window.

The further steps will depend on the selection you have made. In order to continue using the wizard, press the **Next** button.

If no additional settings configuration is required, the **Finish** button will become enabled. In order to complete the wizard, press this button.

5. If you selected disinfection as the action to be performed with the object, in the next you will be offered to determine the procedure to be used to process objects that could not be disinfected (see Figure 18).

Select the option required from the list in the wizard window and press the **Finish** or the **Next** button.

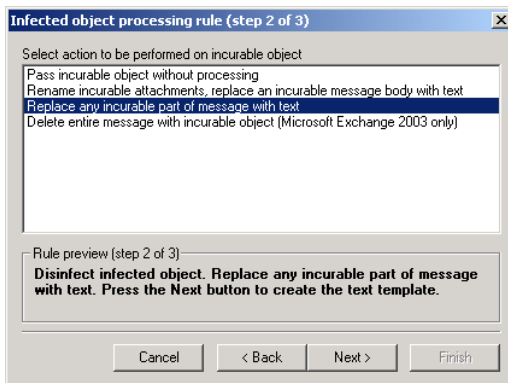


Figure 18. Selecting an action to be performed with an object that could not be disinfected.

6. If you selected one of the actions that involves replacement of the object with text, you will be offered to create a replacement template (Figure 19). The informational message created based on this template will be copied to the message body and into the replacement txt file.

Create a replacement template. In order to do this, enter the message text into the wizard window. The text of this notification may include information about the virus detected and about the infected object. To include this information add corresponding substitution macros to the template selecting them from the dropdown list accessible via the **Macros** button. A detailed description of macros is provided in Appendix A, page 126.

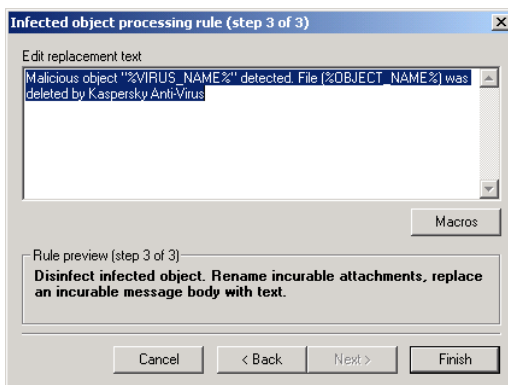


Figure 19. Creating a replacement template

In order to close wizard, press the **Finish** button.

7. In order to ensure that a copy of the object is saved to the backup storage before the object is processed, check the **Save a copy of the original object in the backup storage** box.
8. In order to apply the changes, press the **Apply** or the **OK** button.

5.5. Anti-virus protection efficiency

Kaspersky Anti-Virus provides the possibility to fine-tune the application's operation efficiency depending on the amount and the characteristics of the mail traffic through the Exchange servers and on the system features of the computer: amount of RAM, operation speed, number of processors, etc.

The efficiency settings may be configured either in the automatic or in the manual mode.



In order to configure the application's operation efficiency settings

1. In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **Additional settings** tab in the **Anti-virus protection** window (see Figure 20) that will open.
3. In the **Performance settings** group of fields select the desired method: **Automatic configuration** or **Manual configuration**.
4. If you selected automatic configuration, move the slider located below to the position that corresponds to the characteristics of the mail traffic through your Exchange server:
 - **Small e-mail flow** – this option is provided for the conditions when the server is servicing a large number of mailboxes, but the number of messages to each of them is inconsiderable.
 - **Intensive e-mail flow** – corresponds to the situation when there only a few mail boxes, but there are a great number of e-mail messages sent to each of the mailboxes.
 - Middle position of the slider corresponds to the situation of even distribution of messages among server mailboxes.

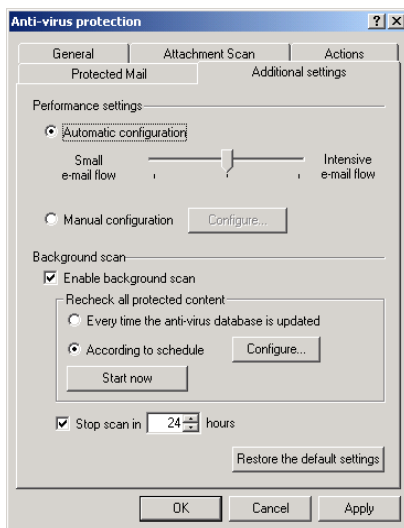


Figure 20. Configuring the efficiency of the anti-virus protection

5. If you selected manual configuration you will have to specify the settings determining the level of the application's efficiency. In order to do this press the **Configure** button and specify the following information in the **Efficiency** window that will open (see Figure 21):
 - The number of streams that contain objects to be scanned (the default value is 3). Microsoft recommends that the value of this setting equals the *number of processors x 2 + 1*.
 - The number of instances of the anti-virus kernels running at the same time (the default value is 4).
 - Specify whether the application must scan objects in RAM without first saving these objects in the temporary folder. In order to enable this mode, check the Scan in RAM objects not large than and specify the maximum size in kilobytes. By default, the box is checked and the size of the object is 1024 KB.
 - To apply the changes press the **OK** button.
6. In order to apply the changes, press the **Apply** or the **OK** button.

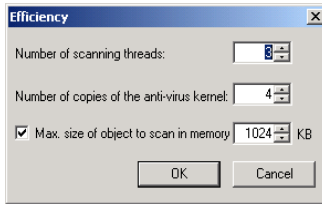


Figure 21. Configuring the anti-virus protection efficiency in the manual mode

5.6. Background scan

Kaspersky Anti-Virus scans mail stored on the server and the content of the public folders (including all public folders and protected mailbox storages). Only those messages that had not been scanned with the current (latest) version of the anti-virus database will be scanned. The application scans the body of the message and attached files in accordance with the general settings of the anti-virus scan.

If background storage scan is disabled, e-mail messages stored on the server will be scanned only when a particular e-mail message is requested by the user. In this case, such e-mail message will be scanned immediately before the delivery.



Only mailboxes located in the protected storage areas will be scanned.



In order to ensure that Kaspersky Anti-Virus scans e-mail messages stored on the server and the content of public folders,

1. In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **Additional settings** tab in the **Anti-virus protection** window (see Figure 22) that will open.

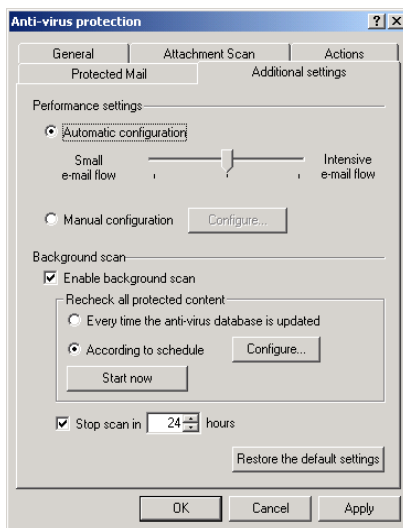


Figure 22. Configuring background scan settings

3. Check the **Enable background scan box** (unchecked by default) and specify the desired scan launch option:
 - **Each time anti-virus database is updated** – every time the anti-virus database is updated.
 - **Scheduled scan** – according to the specified schedule.

If you need to launch the scan immediately, press the **Scan now** button.

4. If you selected the scheduled scan launch option, you will have to create the schedule. In order to do this, press the **Configure** button and specify the mode and the start time for the scan in a window that will open (see Figure 23).

You can restrict the scan time. In order to do this, check the **Stop scan in [NN] hours** box and specify the desired time period in hours. After this period of time (24 hours by default) expires, the scan will be stopped.

5. In order to apply the changes, press the **Apply** or the **OK** button.

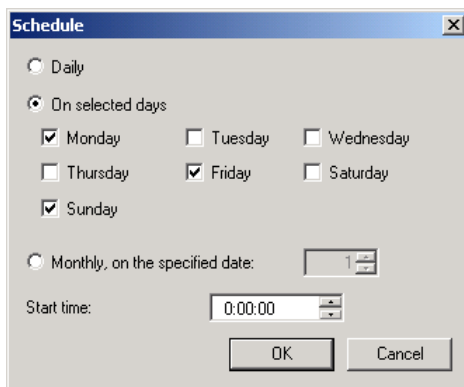


Figure 23. Creating the background scan schedule

CHAPTER 6. UPDATING THE ANTI-VIRUS DATABASE

Users of Kaspersky Lab's products can update the anti-virus database used by their Kaspersky Anti-Virus to detect malware and to disinfect infected objects.

As new viruses are created daily, it is extremely important that you maintain your anti-virus database up-to-date. We recommend that you update your anti-virus database immediately after your application is installed because the bases included into the distribution kit will be out-of-date by the moment when you install your application.

The application copies anti-virus database updates via internet from the Kaspersky Lab's update servers or from a network updates folder. The use of the particular resource depends on the settings.

Updates are downloaded either according to the schedule or manually. In order to download updates from the internet, your computer must have an internet connection. Kaspersky Anti-Virus downloads updates from the dedicated update servers and then installs the required file on your computer.

Information about the anti-virus database version used by the application and about the results of the last update is accessible via the [Anti-virus updates](#) link in the **General** tab of the **Anti-virus Updates** window. The following information is provided:

- date on which the anti-virus database was created on the Kaspersky Lab's HTTP and FTP servers;
- number of records in the anti-virus database;
- results of downloading of the current version of the anti-virus database from the updates source.



In order to update the Kaspersky Anti-virus database

1. In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-virus updates](#) link in the results pane.
2. Specify the source of updates in General tab of the **Anti-virus updates** window (see Figure 24) that will open. You can select update from the internet or from the network folder (details see para 6.1, page 62 and para 6.2, page 64).

- For automatic updates, create an updates downloading schedule (details see para 6.3, page 66). If updates are required immediately, press the **Update now** button (details see para 6.4, page 67) to download the updates manually.



Before performing manual updating, make sure that all settings are configured correctly.

- After the settings are configured press the **Apply** or the **OK** button.

You can restore the default settings by pressing the **Restore default settings** button.

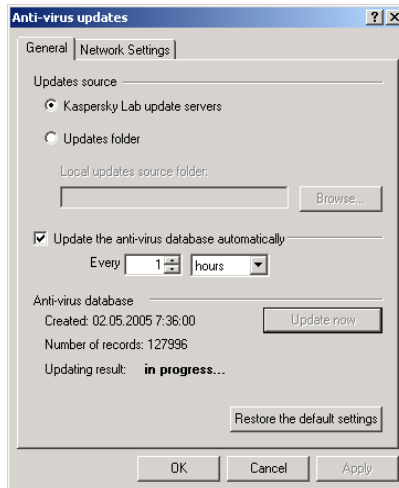


Figure 24. Anti-virus database updates settings window

6.1. Downloading updates from the internet



To receive anti-virus database updates from the Kaspersky Lab's HTTP and FTP servers via internet,

- In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-virus updates](#) link in the results pane.

2. Go to the **General** tab in the **Anti-virus updates** window that will open and select **Kaspersky Lab update servers** (default option) as the source of updates.

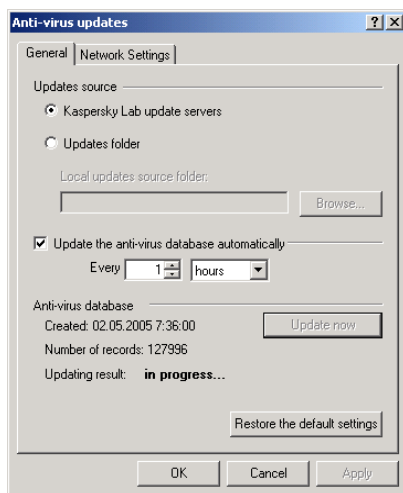


Figure 25. Configuring internet updates downloading

3. After this, configure the network connection settings in the **Connection settings** tab (see Figure 26).

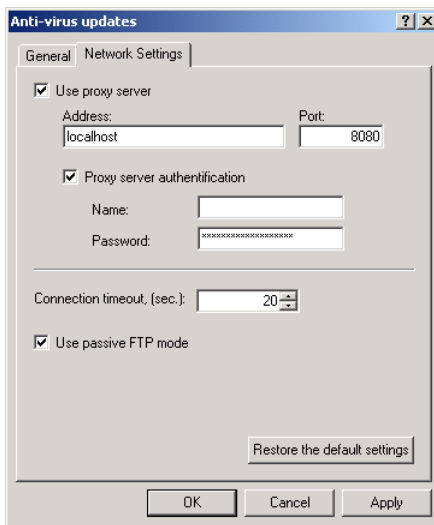


Figure 26. Configuring the network connection settings

- If you connect to the internet using a proxy server, check the **Use proxy server** box and specify the connection settings: connection port address and number.

If you have to use a password to access the proxy server, specify the proxy server authorization parameters by checking the **Use proxy server authentication box** and filling the **Username** and the **Password** fields. By default Microsoft Internet Explorer connection settings will be used.

- Specify time limit for establishing connection with the update server in the **Connection timeout (sec)** field. If the connection was not established within the specified time limit, the application will attempt to establish connection to the next update server until the connection is established or until all servers will be tried for connection.
 - If you would like to use the passive mode for updating from an FTP server, check the **Use the passive FTP mode** box, if you need to use the active mode – uncheck this box. We recommend using the passive mode.
4. After you are done with the settings press the **Apply** or the **OK** button.

You can restore the default settings by pressing the **Restore the default settings** button.

6.2. Downloading updates from a shared network folder

If you use the Kaspersky Administration Kit 5.0 centralized management system to control Kaspersky Lab's applications installed on your network computers, then the anti-virus updates received by the Administration Server will be copied into a dedicated shared folder (details see Kaspersky Administration Kit 5.0 Guide). You can use this folder as the updates source for the Kaspersky Anti-virus database.



In order to ensure correct updating, the computer, on which the Security Server is installed, should have rights to read from the shared network folder.



In order to ensure that Kaspersky Anti-Virus receives the anti-virus database updates from the shared network folder,

1. In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node

- corresponding to the server you need and follow the [Anti-virus updates](#) link in the results pane.
2. Go to the **General** tab in the **Anti-virus protection** window that will open (see Figure 27), select the **Updates folder** as the updates source and specify the path to the required network or local folder. You can enter the path manually or select it using the **Browse** button in the standard Windows **Select folder** dialog box (see Figure 28).
 3. After you are done with the settings press the **Apply** or the **OK** button.

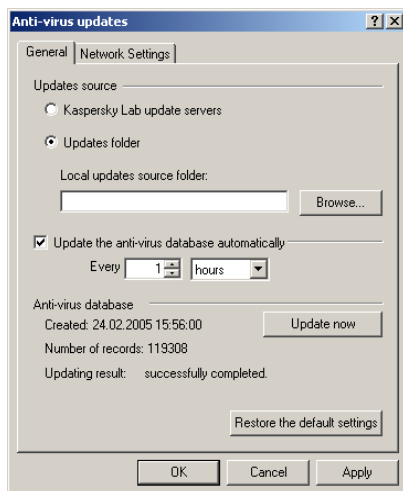


Figure 27. Updates settings from the local folder

You can restore the default settings by pressing the **Restore the default settings** button.

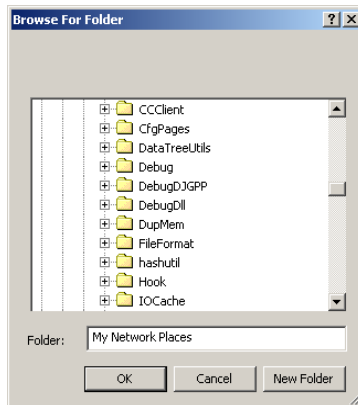


Figure 28. Selecting the updates folder

6.3. Automatic updates



In order to update the anti-virus database in the automatic mode,

1. In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-virus updates](#) link in the results pane.
2. Check the **Update the anti-virus database automatically** box in the **General** tab of the **Anti-virus updates** window (see Figure 29) that will open and create a schedule for receiving the updates. In order to do this specify the required frequency in the **Each** field and select the updates interval from the corresponding drop-down list.
3. After you are done with the settings press the **Apply** or the **OK** button.

You can restore the default settings by pressing the **Restore the default settings** button.

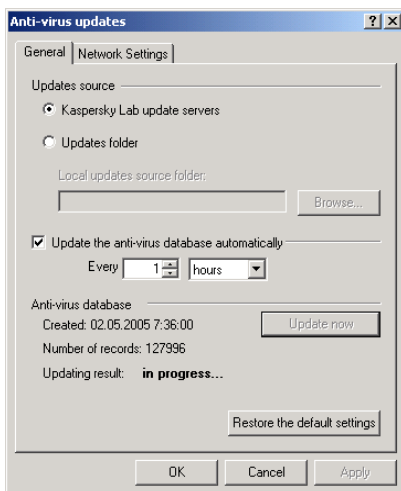


Figure 29. Automatic updates settings

As a result, the application will be automatically updating the anti-virus database at the specified interval and in accordance with the specified settings.

6.4. Manual updating



In order to update the anti-virus database in the manual mode

1. In the main application window select the **Microsoft Exchange Servers** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-virus updates](#) link in the results pane.
2. In the **General** tab in the **Anti-virus updates** window (see Figure 29) that will open press the **Update now** button.

As a result, the application will perform immediate updates of the anti-virus database in accordance with the specified settings.

CHAPTER 7. BACKUP COPYING

Kaspersky Anti-Virus allows saving a backup copy of an infected object before processing. A copy of such object is created in the *backup storage*. Later objects located in the backup storage may be:

- **restored** This feature may prove very useful, for example, if during the disinfection process some data were lost or if the object was deleted by mistake or if another disinfection attempt is required using updated anti-virus database. Details see 7.3, page 72.
- **sent to Kaspersky Lab for analysis.** For example, this feature can be used if the infected object could not be disinfected. Kaspersky Lab's experts may be able to detect a virus not known before and its description will be then included into the updated anti-virus database. In this case, processing of such object, that will be performed later, using the updated anti-virus database, will allow to disinfect the object and keep the integrity of the data it contains. Details see para 7.4, page 74.
- **deleted** Details see para 7.5, page 75.



A backup copy of the object will be created only if it is provided for by the selected anti-virus protection parameters: box **Save a copy of the original object in the backup storage** box on the Actions tabs of the Anti-Virus protection window (see Figure 16) is checked (details see para 5.4, page 51).

The object is stored in the backup storage in the encrypted form, which ensures:

- no risk of infection (object is not accessible without decoding);
- saving time for the anti-virus application (encrypted files stored in the backup storage are not identified as infected).

The backup storage is a service folder on the server disk file system. By default the backup storage folder's name is **qb**. It is created in the application's installation folder during the installation of the **Security Server** component. Any other folder selected by the administrator can be used as the backup storage (details see para 7.6, page 75).

Data that can be stored in the backup storage may be restricted by one of the two following parameters: backup storage size or objects storage period. By default, the size of the backup storage is limited, the maximum size is 50 MB. The administrator can alter the restriction parameter used as well as its value (details see para 7.6, page 75).

The compliance with the restrictions is checked when a new backup copy is saved to the backup storage. The application performs the following actions:

- if the backup storage size is limited and there is not enough space to save the new object, the application will free the required space by removing the "oldest" objects;
- if the object storage period is limited, the application will delete objects with the expired storage period.



The object can stay in the backup storage longer than the established storage period if no new objects are added to the storage.

Viewing the backup storage (details see para 7.1, page 69), configuring backup storage parameters (details see para 7.6, page 75) and managing backup copies (details see para 7.3, page 72, para 7.4, page 74 and para 7.5, page 75) features are available via the Backup Storage service folder (see Figure 30). This folder is included into the structure of each node reflecting the managed Exchange server.

For convenient viewing and searching for data in the backup storage and for data structuring purposes a custom filters configuration capability is provided (details see para 7.2, page 70). Filters, created for the backup storage, can be viewed in the **Backup Storage** folder as subfolders under names assigned by the administrator when the filters were created.

7.1. Viewing backup storage



In order to view the backup storage

select the **Backup Storage** folder in the console tree.

After this a table containing the full list of all objects contained in the backup storage will appear in the results pane (see Figure 30)

Name	Object status	Detected	Type	From	To	Cc	Subject	Sent	Storage
Inb...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		bases	10.0...	C:\Progr...
Inb...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		bases	10.0...	C:\Progr...
Unc...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Unc...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
EIC...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Cur...	Disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Unc...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
EIC...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
EIC...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
EIC...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Cur...	Disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Unc...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
EIC...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Cur...	Disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...
Unc...	Not disinfected	10.05.20...	Atta...	Admi...	Ad...		HTML...	10.0...	C:\Progr...

Figure 30. Viewing backup storage

In addition to the standard e-mail message attributes (**From, To, Cc, Subject, Time sent**), this table will contain the following information for each object:

- **Name.** Attachments will retain their original names, while the message body will be saved as **<message body>**.
- **Object status.** The status assigned to the object as a result of an anti-virus scan or of a disinfection attempt: **not disinfected, disinfected, suspicious, protected or corrupted** (details see para 5.4, page 51).



The application places into the backup storage a **copy of an object before** this object is processed by the Anti-Virus. The **Status** field displays the object status **after** processing.

- **Detected.** Exact date and time when the object was detected by Kaspersky Anti-Virus.
- **Type.** The type of the object saved to the backup storage (Message body or Attachment) indicates where the infected object was detected.
- **Storage folder.** Path to the disk folder where the backup copy is stored.

You can perform ascending and descending sorting of the data contained in the table by any column.

7.2. Backup storage filter

The use of filters allows perform search and data structuring tasks on the data contained in the backup storage as after applying the filter only information complying with the filtering parameters becomes available. This feature becomes very important as the number of objects stored in the backup storage increases. The filter can be used, for example, to search for objects that must be restored.



In order to create a backup storage filter:

1. Select the **Backup Storage** folder in the console tree and use the **Filter** command in the shortcut menu or the analogous item under the **Action** menu. This will open the filter settings window.
2. Specify the name under which the filter will be saved in the **Backup Storage** folder.

3. Specify the parameter values that will be used to perform the search for (filtering of) objects stored in the backup storage. The following object attributes are used to configure the parameters:
 - object status (multiple values can be selected);
 - object name;
 - message sender;
 - message recipient;
 - message subject;
 - time interval, during which the message was sent
4. After you are done with the filter settings, press the **Apply** or the **OK** button to create the filter. If you wish to cancel creation of the filter, press the **Cancel** button.

As a result of this action, a subfolder with the filter's name will be created in the console tree inside the **Backup Storage** folder. When the filter is selected in the console tree, only data that comply with the filter criterion will be displayed in the results pane.

Later you can alter then filter parameters value or delete the filter using the shortcut menu commands or the **Action** menu commands.



In order to change the filter parameters:

1. Select the filter you need to modify in the **Backup Storage** folder in the console tree and use the **Properties** command in the shortcut menu or the analogous item under the **Action** menu. This will open a filter settings configuration window (see Figure 31).
2. Modify the filter parameter values as required.
3. In order to apply the changes, press the **Apply** or the **OK** button. For exit without saving the changes made, press the **Cancel** button.

As a result, the information displayed in the results pane will be updated according to the new values of the filter settings.

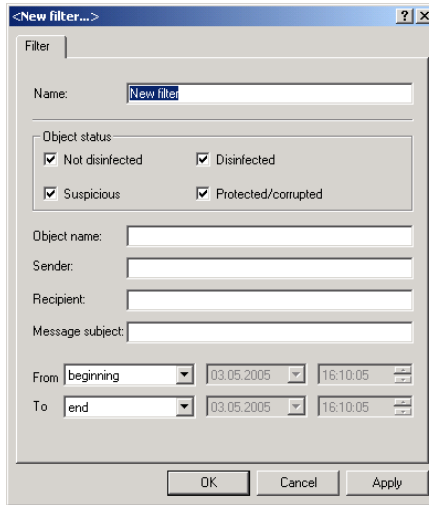


Figure 31. Creating a filter



In order to delete a filter:

Select the **Backup Storage** folder in the console tree and use the **Filter** command in the shortcut menu or the analogous item under the **Action** menu.

As a result of these actions the filter will be removed from the **Backup Storage** folder.



When the filter is deleted, no objects are removed from the backup storage. Objects that meet the filter parameter will still be available in the **Backup Storage** folder.

7.3. Restoring objects from the backup storage



In order to restore an object from the backup storage:

1. Select the **Backup Storage** folder in the console tree.

2. Select the object you wish to restore in the table displaying the content of the backup storage (see Figure 30). You can use filter for searching for the object (see para 7.2, page 70).
3. Open the shortcut menu and use the **Get file** or the analogous command under the **Action** menu.
4. In a window that will open (see Figure 32) specify the folder to which you wish to save the object restored, and if required, enter or modify the object's name.
5. Before sending a warning message (see Figure 33) will be displayed and ask you to confirm that you wish to proceed with the restoring. Press the **Yes** button to restore the object.

As a result of these actions the object will be moved from the backup storage into the specified folder, decoded and saved with the specified name. The restored file will have the same format as it had when it first processed by Kaspersky Anti-Virus. After the object is successfully restored, a corresponding notification is displayed on the screen.



We recommend restoring only those objects that have **suspicious, protected or corrupted** status. A new scan of such objects using the updated anti-virus database may result in the change in their status: the object may be disinfected or a new virus unknown before may be found in this object.

Restoring other objects may result in infecting your computer!

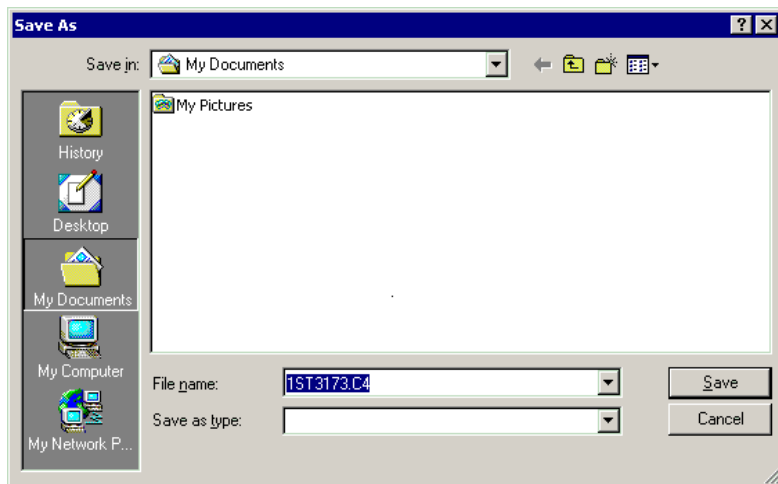


Figure 32. Restoring objects from the backup storage



Figure 33. Confirming object restoring

7.4. Sending objects for analysis



In order to send an object from the backup storage to Kaspersky Lab's experts for analysis,

1. Select the **Backup Storage** folder in the console tree.
2. Select the object you wish to send for analysis in the table displaying the content of the backup storage (see Figure 30). You can use filter when searching for the object (see 7.2, page 70).
3. Open the shortcut menu and use the **Send for analysis** or the analogous command under the **Action** menu.

As a result of these actions an e-mail message with the selected object attached will be created on the computer where the managed Exchange server is installed, and this message will be sent to Kaspersky Lab.

After the message is sent a message confirming the file has been sent will be displayed by the computer from which the control is maintained (see Figure 34).

If the restoring succeeded, you can delete the object from the backup storage (see para 7.5, page 75).

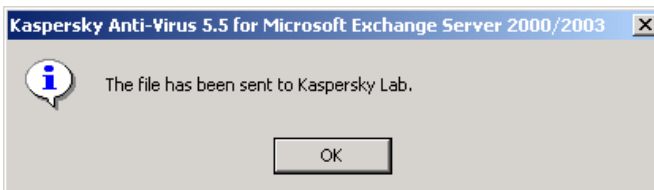


Figure 34. Message confirming the object has been sent for analysis

7.5. Deleting objects from the backup storage

The following objects are automatically deleted from the backup storage:

- "older" objects if there is a restriction imposed on the backup storage size and for there is not enough space for storing a new object. The application will delete the number of older objects required to free the space needed.
- objects whose storage period has expired, if there is a restriction imposed on the storage period.

A possibility to manually remove objects from the backup storage is also provided. This feature may prove useful to delete objects that have been successfully restored or sent for analysis and to free space in the backup storage if the automatic object removal methods did not help.



In order to manually delete an object from the backup storage,

1. Select the **Backup Storage** folder in the console tree.
2. Select the object you wish to delete in the table displaying the content of the backup storage (see Figure 30). You can use filter when searching for the object (see 7.2, page 70).
3. Open the shortcut menu and use the **Delete** or the analogous command under the **Action** menu.

As a result of these actions, the object will be deleted from the table reflecting the content of the backup storage.

7.6. Configuring the backup storage settings

The backup storage is created during installation of the **Security Server** component. The settings of the backup storage are determined by default and can be altered by the administrator.



In order to modify the backup storage parameters,

1. Select the **Backup Storage** folder in the console tree.
2. Open the shortcut menu and use the **Properties** or the analogous command under the **Action** menu.

3. In the **Backup Storage properties** window that will open (see Figure 35) select the required settings values.

In order to change the folder where the backup storage is located, type the path to the new folder and the folder name in the **Backup Storage folder** field or specify the corresponding folder using the **Browse** button (see Figure 36)

By default, the backup copy of the object is stored in **qb** folder. This is a service application folder, which is created ins the application installation folder at the time when the Security Server is installed. When you change the backup folder, backup copies that had been created earlier will remain the folder they had been placed initially. Objects from all folders are removed automatically based on the application restriction selected.

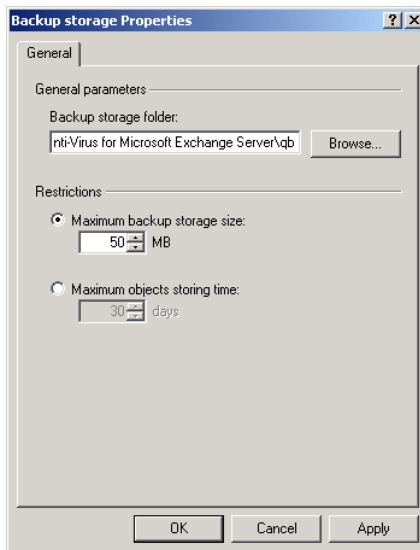


Figure 35. Configuring the backup storage settings

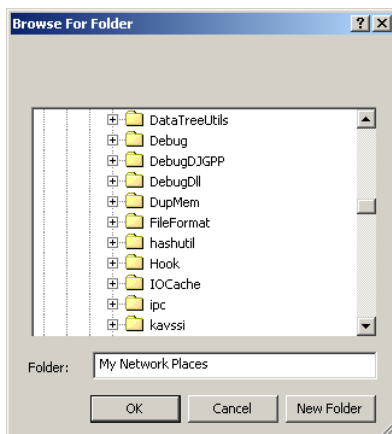


Figure 36. Changing the backup storage folder

In order to impose a restriction, select one of the options and enter the required value for the selected setting as follows:

- **Maximum storage size** – if you wish to restrict the total size of objects located in the backup storage (default option), specify the value in the entry text field (the default value is 50 MB). During the calculations, the total size of all objects is summed up no matter which folder a particular object is stored in.
 - **Maximum object storage period** – if you wish to restrict the period objects are stored in the backup storage (unlimited by default), specify the number of days in the entry field (the default value is 30 days).
4. In order to apply the changes, press the **Apply** or the **OK** button. For exit without saving the changes made, press the **Cancel** button.

CHAPTER 8. NOTIFICATIONS

Kaspersky Anti-Virus allows to notify about infected objects detected during the anti-virus scan.

The following types of notifications are provided:

- infected object detected;
- suspicious object detected;
- corrupted object detected.

A notification of the corresponding type is created for each type of event

- Notification about an infected object;
- Notification about an infected object
- Notification about a corrupted object.

Notifications can be delivered using several methods:

- by sending e-mail messages;
- by sending messages using Net Send tools;
- by registering the event in the **Windows** system log on the computer where the Security Server component is installed.

In this case, access to the information will be provided using **Events Viewer**, a standard **Windows** tool used for viewing and managing logs

There is a possibility to notify the sender and the recipient of the message about the infected object.



Recipients of blind carbon copies (Bcc) are not notified about infected objects.

The procedure used for notification, the method of distribution and the text of the messages sent are created by the administrator in the form of a notification template.

When a certain event happens, a automatic notification of the corresponding type is issued based on such template.

Several templates of the same type but with different parameter values may be created which allows to create notifications to the administrator, sender, recipient and security services that vary as far as the content and the delivery method are concerned,

By default, no notifications are issued about infected objects detected. However, during the installation of the Security Server a built-in notification template is created. Based on this template notifications can be configured.

Notification templates are stored in the **Notification templates** service folder. This folder is included into each node that reflect the managed Exchange server.

The list of created notification templates is provided in the form of a table (see Figure 37). The table contain the name of the template and notification type for each template.

You can learn more about templates parameters in the settings window that opens by the **Properties** command available through the shortcut menu (details see para 8.1, page 79).

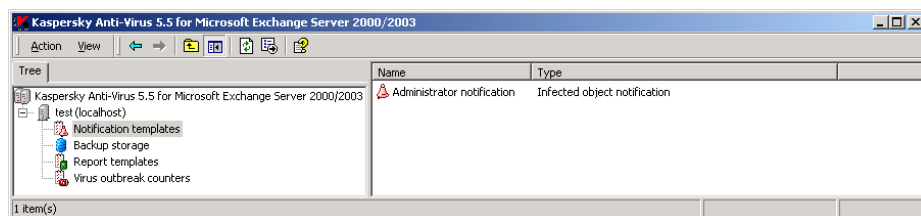


Figure 37. The **Notifications** folder

The administrator can create new templates, view and edit parameters of the existing templates and rename or delete templates using the shortcut menu commands.



In order to enable notification about infected objects detected during the anti-virus scan.

1. Create a notification template (see para 8.2, page 82) or select an existing template and configure its settings (see para 8.1, page 79).
2. Check the **Notify about events** box in the **General** tab of the notification template settings dialog box (see Figure 38).

8.1. Viewing and editing notification parameters



In order to view or modify notification parameters,

1. Select the **Notification templates** folder in the console tree.

2. Select the required notification template in the table containing the list of created templates (see Figure 30).
3. Open the shortcut menu and use the **Properties** command or the analogous command under the **Action** menu.
4. As a result of these actions a notification template settings windows will open Properties: <Template name> (see Figure 38). The window consists of tabs General, Text, Action and is completely similar to the New Notification Properties (see Figure 41). parameters are changed the same way they are specified when the notification was created (details see 8.2, page 82).
5. You can view and modify name of the template, description and type of notification in the **General** (see Figure 38) tab and specify whether the notification based on this template will be performed or not. If the **Notify about events** box is checked, notifications based on this template will be issued, otherwise – not.

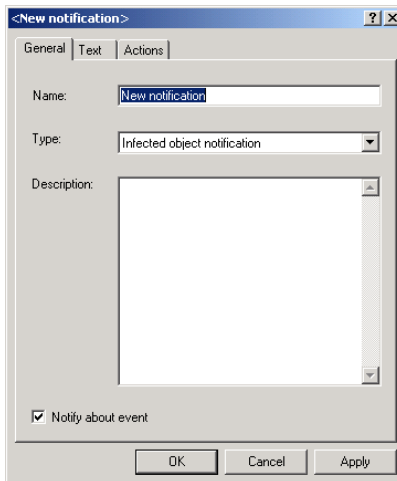


Figure 38. Modifying notification template. The **General** tab

You can view the template of the message that is sent as a notification and modify its parameters on the **Text** tab (see Figure 39),

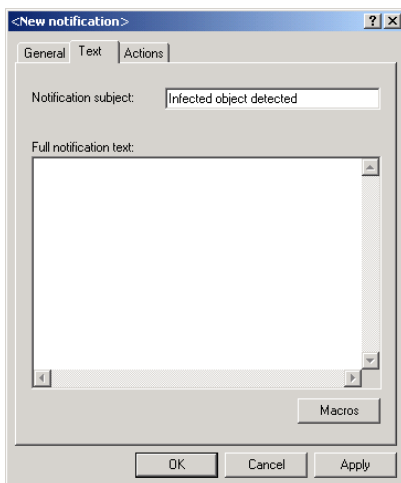


Figure 39. Modifying notification template. The **Text** tab

The **Actions** tab (see Figure 40) contains notification methods, recipients and computers that receive notification messages (if the corresponding notification options have been selected). You can select other methods of notification and modify the parameter values.

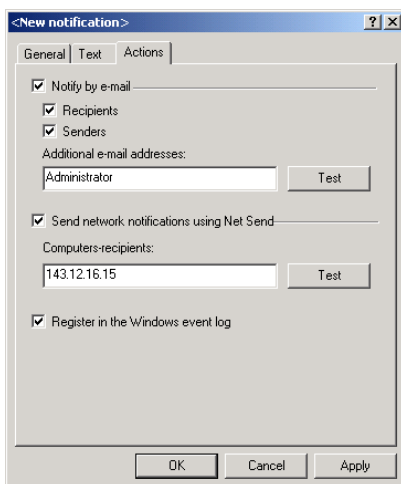


Figure 40. Modifying notification template. The **Actions** tab

6. After you have made the changes, press the **OK** or the **Apply** button to apply changes. For exit without savings the changes made press the **Cancel** button.

8.2. Creating a notification template



In order to create a new notification template:

1. Select the **Notification templates** folder in the console tree
2. Open the shortcut menu and use the **New template** command or an analogous command under the **Action** menu.
3. As a result of these actions a **<New notification>** windows used for configuring new notification template will open (Figure 41). Specify the required values for the parameters in the tabs of the window.

Perform the following actions on the **General** tab (see Figure 41):

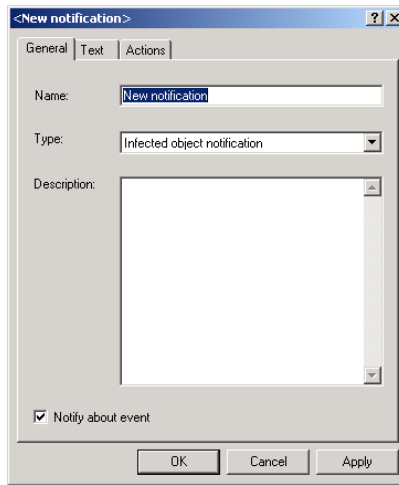


Figure 41. Notification template. The **General** tab

- Enter the template name in the **Name** field.
- Specify the notification type. It must match the event which would trigger the notification to be created.

In order to specify the type, select the required value from the **Type** drop-down containing the following values.

- **Infected object notification.**
- **Suspicious object notification**
- **Corrupted object notification**
- If necessary, enter a more detailed description of the notification in the **Description** field.
- Determine whether notifications will be created based on this template.

In order to do this check (or uncheck) the **Notify about event** box.

Create a template of the message that will be sent as a notification on the **Text** tab (see Figure 42):

- Enter a brief description of the notification in the **Notification Subject** field. This line will be used as the header of the message.
- Create the message text in the **Full notification text** field. The message may include information about a registered event. To include this information add corresponding substitution macros to the template selecting them from the dropdown list accessible via the **Macros** button. The full list of the substitution macros is provided in Appendix A, page 126.

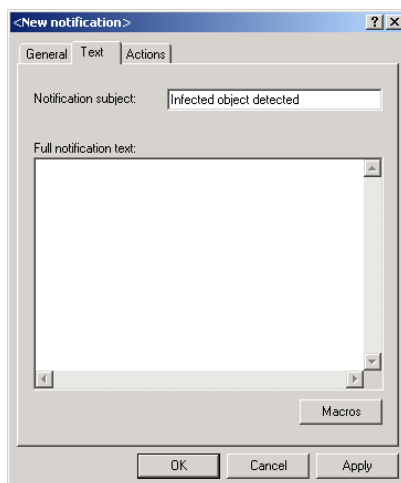


Figure 42. Notification template The **Text** tab

Select the notification method and specify the corresponding parameter values in the Actions tab (see Figure 43) The application provides for several methods to be used.

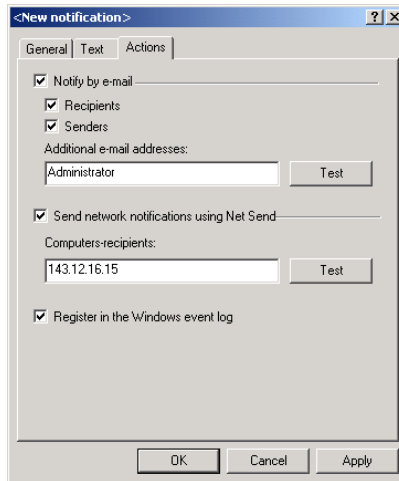


Figure 43. Notification template The Actions tab

- In order to send messages via the mail server, check the **Notify by e-mail** box and specify the recipients' addresses the mailing.
 - In order to notify recipients an senders of the infected message about infected objects detected, check the **Recipients** and **Senders** boxes.
 - In order to notify other users, as for example, administrator, enter his or her e-mail address in the **Additional e-mail addresses** field.

The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.

Entering several e-mail addresses is allowed, the addresses entered must be separated by semicolons.

- In order to send messages via network using the Net Send service, check the Send network notifications using Net Send box and specify the addresses of the computers-recipients in the Computers-recipients field

IP address or NetBIOS-computer name can be used as the computer address.

The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.

Entering several e-mail addresses is allowed, the addresses entered must be separated by semicolons.

- In order to register events in the Windows system log, check the **Register in the Windows event log** box.
4. After you are done with the settings press the **Apply** or the **OK** button.

As a result of these actions the notification template will be added to the **Notification templates** folder and will be included in the table displayed in the results pane and, if the **Notify about events** box in the **General** tab is checked, notifications will be issued using this template.

CHAPTER 9. PREVENTING VIRUS OUTBREAKS

Kaspersky Ant-Virus allows to detect increases in the virus activities on the protected Exchange server and to notify the administrator and other users about such events. This feature is of great significance in the periods of virus outbreaks as it helps the administrator timely react on the emerging threats of virus attacks.

Virus activity level is determined based on the server anti-virus protection data and allows registering events of the following types:

- An infected object detected
- A suspicious object detected
- A damaged object detected
- One and the same virus detected several times

The administrator specifies the virus activity level threshold– a maximum allowable number of events of the specified type within a certain limited time interval. If the virus activity level is greater than the specified threshold, a notification will be issued.

Notifications can be delivered using several methods:

- by e-mail messages;
- by messages sent over the network using Net Send;
- by registration of the event in the **Windows** system log on the computer where the **Security Server** component is installed.

In this case, the information is accessible through the use of **Events Viewer**, a standard Windows logs viewing and management tool.

The virus activity level threshold, notification procedures, delivery method and the text of messages sent are determined by the administrator in the *virus outbreaks counter* settings.

If the specified virus activity level threshold is exceeded, a notification about the threat of a virus outbreak will be issued based on the settings of the virus outbreaks counter. Upon the expiration of a specified period, the counter's values will be reset.



The values of all virus outbreak counters will be reset if the Security Server component or the server operating system, where the component is installed, are restarted.

Several counters with different settings values can be created for each type of events.

By default, notifications about increased virus activity level are not issued. However a built-in virus outbreaks counter is created during the installation of the Security Server. Virus outbreak notification can be set up based on the counter.

Virus outbreaks counters are located in the **Virus outbreak counters** service folder. This folder is included into the structure of each node reflecting the managed Exchange server.

The list of the virus outbreaks counters created is displayed in the form of a table in the results pane (see Figure 44). The table displays the name of the type for each counter. The counter type corresponds to the type of events traced by this counter.

Detailed information about the virus outbreak counter settings is provided in the settings window accessible through the **Properties** shortcut menu command (details see para 9.1, page 88).

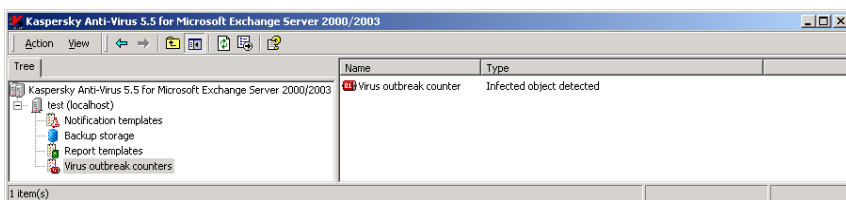


Figure 44. The **Virus outbreaks** folder

The administrator can create new counters, view and edit the settings of the existing counters, rename and delete counters using the shortcut menu commands.



In order to set up issuing notifications about increased virus activity level,

1. Create a new virus outbreak counter (see para 9.2, page 90) or select an existing counter and configure its settings (see 9.1, page 88).
2. Check the **Notify about virus outbreaks** box in the **General** tab of the virus outbreak counter settings (see Figure 45).

9.1. Viewing and modifying virus outbreak notification settings



In order to view or modify the virus outbreak notification settings,

1. Select the **Virus outbreak counters** folder in the console tree.
2. Select the counter you need in the table displaying the list of created counters (see Figure 44).
3. Open the shortcut menu and use the **Properties** or the analogous command under the **Action** menu.
4. As a result of these actions a counter settings window **<Counter name>: Properties** will open (see Figure 45).

This window includes the following tabs: General, Text, Notifications and is completely analogous to the **New counter** window (see Figure 41). Notification settings can be modified the same way as they are specified when the notification is created (details see para 9.2, page 90).

Using the **General** tab (see Figure 45) , you can enable or disable the virus activity level detection feature based on the counter settings and view or modify:

- counter name;
- the type of event the emergence of which is traced by the counter;
- the value of the virus activity level threshold;
- detailed description of the counter.

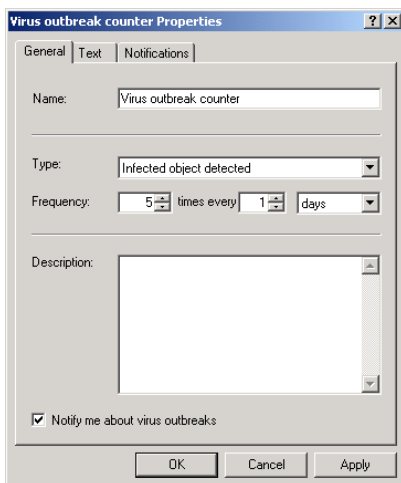


Figure 45. Configuring the virus outbreak counter. The **General** tab

You can view the template of a message sent as a notification or modify its settings in the **Text** tab (see Figure 46).

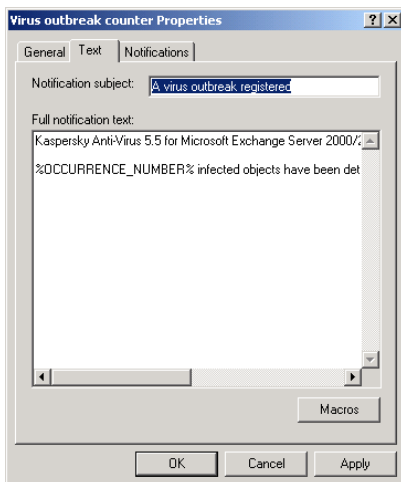


Figure 46. Configuring the virus outbreak counter. The **Text** tab

The **Notification** tab (see Figure 47) contains the methods of delivery, the list of recipients and computers-recipients (if the corresponding notification options are enabled). Here you can select other methods of delivery and modify the settings.

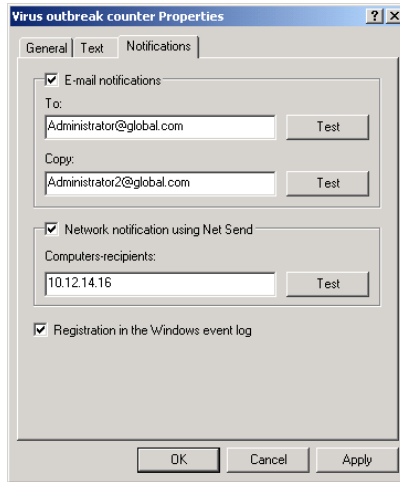


Figure 47. Configuring the virus outbreak counter. The **Notifications** tab.

5. After you have made the changes, press the **Apply** or the **OK** button to apply the new settings. For exit without saving the changes made, press the **Cancel** button.

9.2. Creating a new virus outbreak counter



In order to create a new virus outbreak counter,

1. Select the **Virus outbreak counters** folder in the console tree.
2. Open the shortcut menu and use the **New counter** or the analogous command under the **Action** menu.
3. As a result of these actions, a new virus outbreak counter settings window **New counter** will open (see Figure 48). Specify the required values for the settings displayed in the tabs of this window.

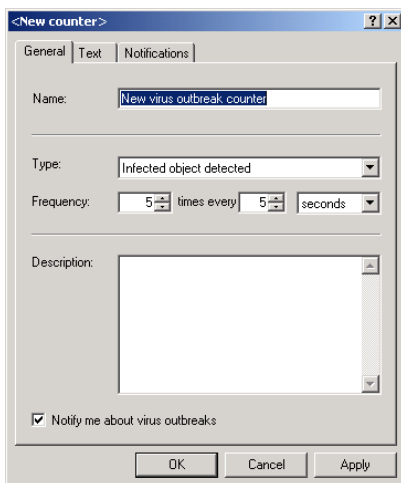


Figure 48. Virus outbreak counter. The **General** tab

Perform the following in the **General** tab (see Figure 48):

- Enter the counter name in the **Name** field.
- Specify the type of the event that will be traced by the counter.
In order to do this, select the required value from the **Type** drop-down list. The list includes the following values:
 - **Corrupted objects detected.**
 - **Suspicious objects detected.**
 - **Viruses detected.**
 - **The same virus detected several times.**
- Specify the value of the virus activity level threshold. In order to do this, specify the values for the settings in the: **Frequency** group using the following order:
 - maximum allowable number of events of the specified type;
 - time period during which these events must be registered;
 - select the time unit **seconds**, **minutes** or **hours**:
- If required, enter a more detailed description of the virus outbreak counter in the **Description** field.

- Specify whether notifications will be issued based on this counter's settings.

Check the **Notify me about virus outbreaks** box if you want a notification to be issued when the virus activity level threshold on the events of the specified type is exceeded. Uncheck this box if you do not want notifications to be issued.

Create the template of a message that will be sent as a notification in the **Text** tab (see Figure 49).



Figure 49. Virus outbreak counter. The **Text** tab

- Enter a brief description of the notification in the **Notification Subject** field. This line will be used as the header of the message.
- Create the message text in the **Full notification text** field. The message may include information about a registered event. To include this information add corresponding substitution macros to the template selecting them from the dropdown list accessible via the **Macros** button. The full list of the substitution macros is provided in Appendix A, page 126.

Select the notification method and specify the corresponding parameter values in the **Notifications** tab (see Figure 50) The application provides for several methods to be used.

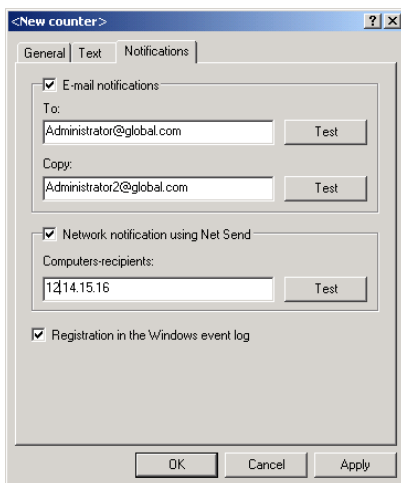


Figure 50. Virus outbreak counter. The **Notifications** tab.

- In order to send messages via the e-mail server, check the Notify by e-mail box and enter the e-mail addresses in the **To** and **Copy** fields.

The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.

Entering several e-mail addresses is allowed, the addresses entered must be separated by semicolons.

- In order to send messages via network using the Net Send service, check the **Network notifications using Net Send** box and specify the addresses of the computers-recipients in the **Computers-recipients** field.

IP address or NetBIOS-computer name can be used as the computer address.

The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.

Entering several e-mail addresses is allowed, the addresses entered must be separated by semicolons.

- In order to register virus outbreaks in the **Windows** system log on the computer where the Security Server component is installed, check the **Registration in the Windows event log** box.

4. After you are done with the settings press the **Apply** or the **OK** button.

As a result:

- the virus outbreak counter will be added to the **Virus outbreak counters** folder and will be displayed as a table in the results pane;
- if the Notify about virus outbreaks box in the General tab is checked, the specified types of the virus activity will be monitored;
- once the specified virus activity level threshold is exceeded, notification about a virus outbreak threat will be issued.

CHAPTER 10. REPORTS

Kaspersky Anti-Virus allows receiving reports about the results of the anti-virus server scan.

Reports contain information registered during a certain period and provide information about:

- infected objects detected;
- viruses found;
- senders of infected messages;
- performance data of the anti-virus scan:
 - the total number of processed objects;
 - average speed of objects processing;
 - maximum speed of objects processing;
 - statistics of infected objects appearance.

Reports are created automatically according to the schedule or manually by request and can be saved in the folder and sent by e-mail. Information contained in the reports saved on disk and those sent by e-mail is identical, however the format, structure and viewing method differ.

Reports saved on disk are created in html-page format and have frame-based structure. They are saved to a folder that contains a predetermined set of files that support frame-based report structure and enable report viewing (details see para 10.2, page 104). This folder is created with the name that reflect the date and the time when the report is created in the following format **<DD.MM.YYYY_HH-MM-SS>**. The default storage location for the reports is the **Reports** folder. It is created in the application's installation folder during the installation of the **Security Server** component. Any other folder selected by the administrator can be used as the report storage (details see para 10.1.1, page 98 and para 10.1.2, page 101). The period for the reports storage on the server and the storage folder size are not limited. Reports are deleted manually using the file system.

Reports sent by e-mail are *him* format files and are sent by mail as attachments. The message contains clarification text as follows: *This message is created by Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003. The attached file contains a report on the anti-virus server scans during the period from: <DD.MM.YYYY_HH:MM:SS> until: <DD.MM.YYYY_HH:MM:SS>*.

Reports are viewed using the default browser.

Reports are created based on the **report templates** created by the administrator. The following is specified in the template: the reporting period, report creation schedule and report format.

By default, the anti-virus server scan reports are not created. However a built-in report template is created during the installation of the Security Server. Creation of reports feature can be configured based on this template (details see para 10.1, page 97).

During Security Server installation the embedded report template is created. Based on this template the server anti-virus scan results report is generated on the first day of each month and covers last 30 days.

Report templates are stored in the **Report templates** service folder. This folder is included into the structure of each node reflecting the managed Exchange server.

The list of the report templates created is displayed in the form of a table in the results pane (see Figure 51).

Apart from the reports' names, this table contains information on the status for each report created based on the template. Depending on current stage of the report creation, the report's status may have one of the following values:

- **being created** – the report is being created (according to the schedule or by request);
- **expected** – creation of the next report is expected based on the schedule;
- **not created** – no reports have been created based on this template (the template have recently been created or reports creation based on this template is disabled).

Detailed information about report template settings is provided in the settings window accessible through the **Properties** shortcut menu command (details see para 10.1.1, page 98).

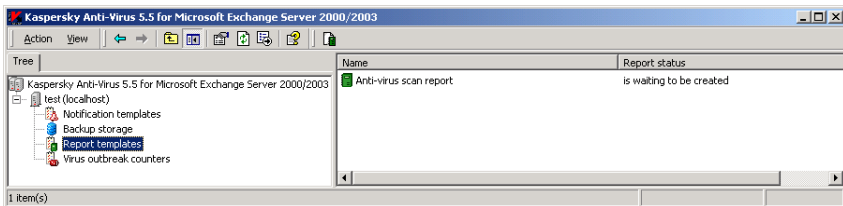


Figure 51. The **Reports** folder

The administrator can create new templates, view and edit the settings of the existing templates, rename and delete templates using the shortcut menu commands.

10.1. Receiving reports



In order to receive an anti-virus server scan report,

1. Create a new report template (see para see para 10.1.2, page 101) or select an existing template and configure its settings (see para 10.1.1, page 98).
2. Check the Create reports box in the General tab of the report template settings window (see Figure 53).

As a result, reports will be created at the time interval specified in the schedule.

In order to view the results of the anti-virus scan, open the report for the corresponding reporting period (details see para 10.2, page 104).

There is a possibility to receive reports by request, irrespective of the scheduled time, which can be useful when you need updated information about the current status of the anti-virus server protection, for example, during virus outbreaks.



In order to receive an on-demand anti-virus server scan report,

1. Select the **Report templates** folder in the console tree.
2. Select the report template you need in the table displaying the list of created templates (see Figure 51)
3. Open the shortcut menu and use the **Create a report** or the analogous command under the **Action** menu.



A report will be created only if creation of reports based on this template is enabled, i.e. if the Create reports box in the General tab of the report template settings window (see Figure 41) is checked.

The report will be created based on the information about the anti-virus server scans results, saved by the application. The application saves all scan results: mail traffic scan results, transit mail results and storage background scan results. In order to reduce the amount of the information stored, a restriction can be imposed on its storage period. By default the information is stored for a period of one year.



In order to restrict the storage period for the anti-virus server results,

1. Select the **Report templates** folder in the console tree.

2. Open the shortcut menu and use the **Properties** or the analogous command under the **Action** menu.
3. In the **Report templates: Properties** window that will open (see Figure 52):
 - Check the **Store the statistical reports data** box.
 - Specify the information storage period and select the time unit in the **Maximum period** group.
4. After you have made the changes, press the **Apply** or the **OK** button to apply the new settings. The settings will change within one hour after the changes have been made. For exit without saving the changes made, press the **Cancel** button.

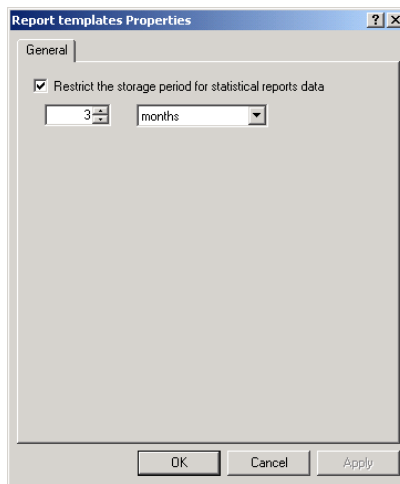


Figure 52. Modifying the reports settings

10.1.1. Viewing and modifying the report templates



In order to view or modify the report template settings,

1. Select the **Report templates** folder in the console tree.
2. Select the report template you need in the table displaying the list of created templates (see Figure 51).

3. Open the shortcut menu and use the **Properties** or the analogous command under the **Action** menu.
4. As a result of these actions, a report template settings window **<Template name>: Properties** will open (see Figure 53).

This window includes the following tabs: **General**, **Parameters**, **Actions** and is completely analogous to the **New report** window (see Figure 41). Template settings can be modified the same way as they are specified when the template is created (details see 10.1.2, page 101).

You can enable or disable creation of reports based on the template, view or modify the template name and its detailed description in the **General** tab (see Figure 53).

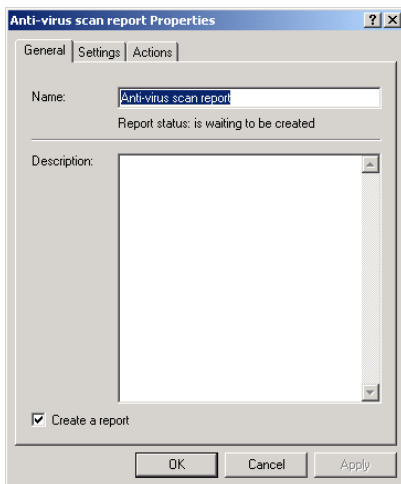


Figure 53. Modifying the report template. The **General** tab

You can view and modify the reporting period and the report creation schedule settings in the **Parameters** tab (see Figure 54).

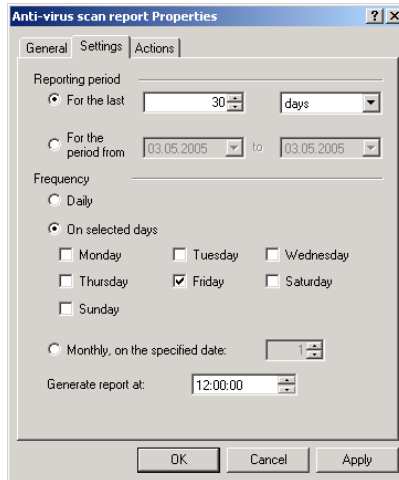


Figure 54. Modifying the report template. The **Parameters** tab.

The **Actions** tab (see Figure 55) contains the reporting methods, the address of the folder where the report is stored and e-mail addresses of the report recipients (if the corresponding reporting method is selected). You can change the reporting methods or modify the values of the settings displayed in this tab.

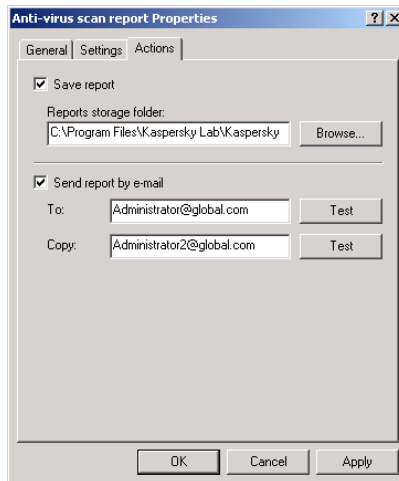


Figure 55. Modifying the report template. The **Actions** tab

10.1.2. Creating a report template



In order to create a new report template,

1. Select the **Report templates** folder in the console tree.
2. Open the shortcut menu and use the **New template** or the analogous command under the **Action** menu.
3. As a result, a report template settings window **New report** will open (see Figure 56) ; this window consists of the following tabs: **General**, **Settings** and **Actions**. Specify the required settings value in the tabs as follows:

Perform the following in the **General** tab (see Figure 48):

- Enter the template name in the **Name** field.
- If required, enter a more detailed description of the report to be created based on this template in the **Description** field.
- Specify whether notifications will be issued based on this template. In order to do this, check (or uncheck) the **Create a report** box.

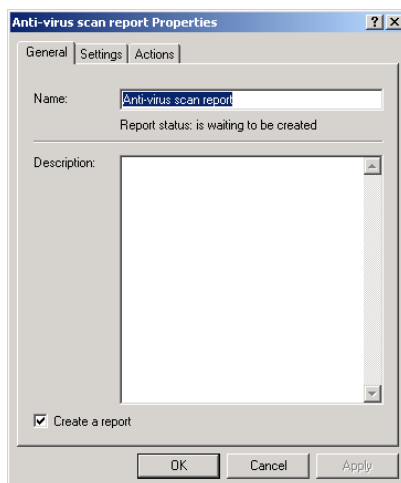


Figure 56. Report template. The **General** tab

Specify the reporting period and the report creation schedule settings in the **Settings** tab (see Figure 57).

- The following options are available when specifying the reporting period:
 - specify the time period. In this case, the report will contain information for the specified period starting with the report creation date and time. In order to set up the reporting period, select **For the last** option in the **Reporting period** group and specify the interval and the time unit (hours, days, weeks, months).
 - specify exact date for the beginning and the end of the reporting period. In order to do this, select **For the period** option in the Reporting period group and specify the desired date in the **From** and **To** fields.
- In order to create a schedule, perform the following in the **Frequency** section:
 - Select the report creation frequency: **Daily, On selected days** or **Monthly, on the specified date**. Configure the schedule settings in accordance with the selected frequency.

If you selected the monthly option as the report creation frequency, reports will be created on the first day of each month.
 - Specify the time when reports will be created in the **Generate report at** field.

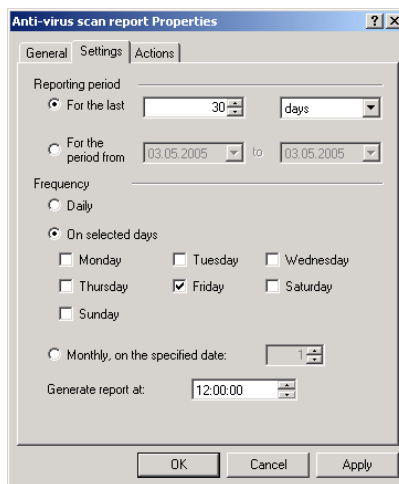


Figure 57. Report template. The **Settings** tab

Specify which format shall be used for reports creation and specify the reports storage folder and mailing list in the **Actions** tab. (see Figure 58).

- In order to create reports and saving them in the server disk file system, check the **Save report** box.

After this, specify the folder into which reports will be saved. By default, the **Reports storage folder**, located on the server in the application installation folder, will be used for storing the reports. You can specify a different folder by typing in the path and the name of the new folder or by using the **Browse** button.

- In order to create and send reports via the e-mail server, check the **Send report by e-mail** box and enter the e-mail addresses in the **To** and **Copy** fields.

The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.

Entering several e-mail addresses is allowed, the addresses entered must be separated by semicolons.

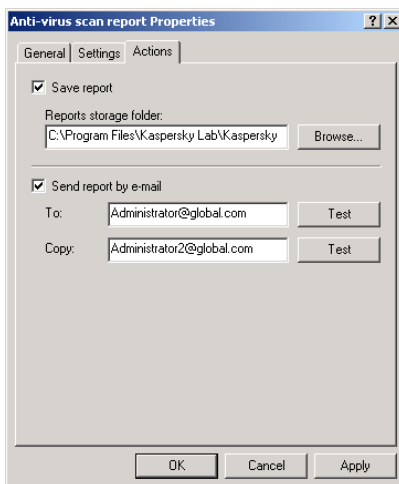


Figure 58. Report template. The **Actions** tab

4. After you are done with the settings press the **Apply** or the **OK** button.

As a result:

- The report template will be added to the **Report templates** folder and will be displayed as a table in the results pane;

- If the **Create reports** box in the **General** tab is checked, the application will create reports according to the time specified in the schedule and with the specified frequency. Reports can also be created by the administrator's request.

10.2. Viewing reports

Depending on the template settings, reports created can be:

- saved in the form of a folder;
- sent by e-mail as an attachment to a message.



In order to view a report saved on disk,

1. Enter the folder where the logs are stored. By default, it is the **Reports** folder located on the server in the application installation folder.
2. Select the subfolder with the name corresponding to the date and time of report creation in the following format **<DD.MM.YYYY_HH-MM-SS>**.
3. Run the *index.htm* file located in the selected subfolder.

As a result the system default browser will be loaded.. The required report about the anti-virus server scan results will be displayed in the main window of the browser (see Figure 59). Immediately after loading, the report displays general results of the scan. The reporting period will be specified in the heading.

Reports have frame-based structure. The left frame contains the list of the report's sections (table of contents), the heading and the content of the selected section are displayed in the right frame.

In order to view a particular section, select this sections name in the table of contents and the content of the section will be loaded in the right frame.

The list of report's sections and the type of information contained in each section is provided in the table below.

Section name	Section content
General scan results	Number of objects detected during the anti-virus scan broken down for each status.
Viruses found:	List of viruses found in the infected object including data on the occurrence of each virus.

Section name	Section content
Senders of infected objects	E-mail addresses of senders of messages in which infected objects were found and the total number of viruses received from each address.
Number of processed objects	The total number of objects scanned by Kaspersky Anti-Virus during the reporting period.
Average speed of objects processing	The number of objects processed per second (average value for the reporting period)
Maximum speed of objects processing	Maximum speed of objects processing per second that was reached during the reporting period.
Statistics of infected objects appearance	The number of infected objects detected per second (average value for the reporting period)

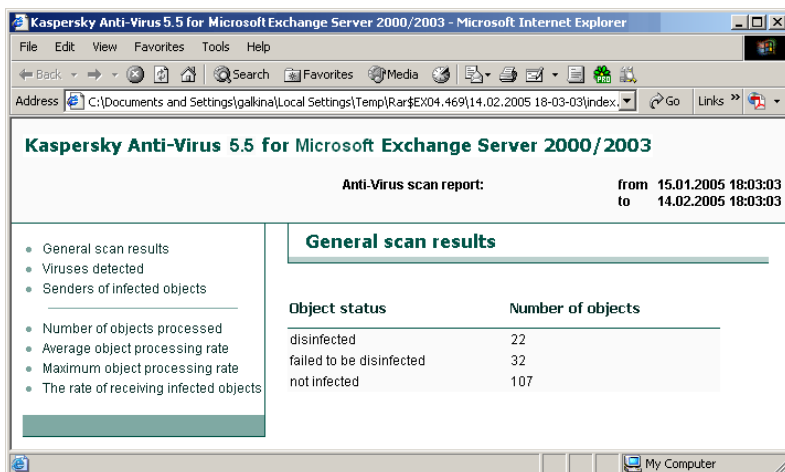


Figure 59. Viewing a report saved on disk



In order to view report delivered by e-mail,

open `index.htm` file attached to the message..

As a result the system default browser will be loaded.. The required report about the anti-virus server scan results will be displayed in the main window of the browser (see Figure 60).

The upper part of the report contains the list of sections (table of contents). This part is followed by the sections including the information they contain. The sections are arranged in the same order as they are listed in the table of contents.

The structure and the content of the sections are identical to those of the report saved to disk.

In order to navigate while viewing the report use the scroll bar of your browser.

In order to move to the beginning of a section, select this section in the table of contents.

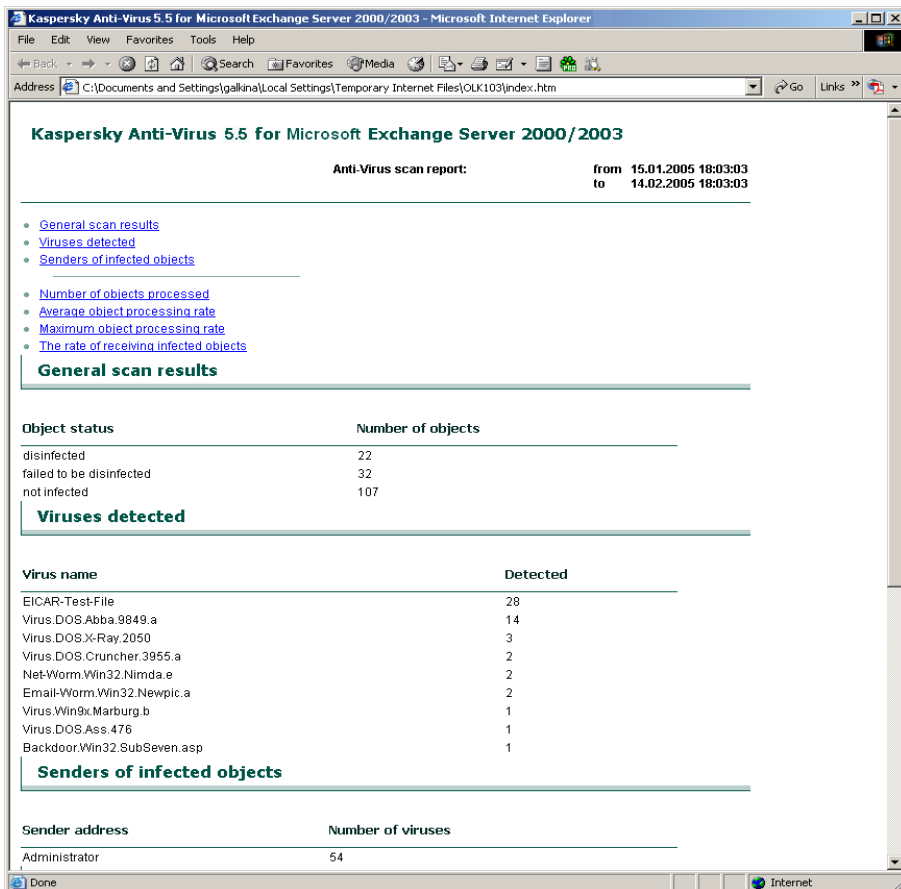


Figure 60. Viewing a report delivered by e-mail

CHAPTER 11. APPLICATION'S EVENTS LOGS

Kaspersky Anti-Virus allows the user to perform full diagnostic of its operation and to register events in the Windows application log and in the Kaspersky Anti-Virus application's log.

The degree of the completeness of the information entered into the logs depends on the diagnostics levels selected in the application's settings (details see para 11.1, page 109).

Events registered in the Windows application log can be viewed using standard Windows tool **Events viewer**. For Kaspersky Anti-Virus the **Source** column will contain line **KAVE**.



To ensure that events registered in the Windows applications log are displayed correctly, a language that matches the language used by your copy of Kaspersky Anti-Virus program must be selected as the Language for non-Unicode programs in the Windows **Regional and Language Options** service

Kaspersky Anti-Virus events logs are maintained in two formats and, depending on the format, the naming conventions for the log files may be as follows:

kavscmesrvDATE.log – main application's events log. The *DATE* part in the filename shall be replaced with the date the log was created on in the **YYYYMMDD** format. For example, *kavscmesrv20050410.log*.

If, by the time when data must be entered into the log, the log is not accessible for writing, for example, if it is open for editing by the administrator, Kaspersky Anti-Virus will create a new file with a postfix added to the filename. For example, *kavscmesrv 20040410_1.log*.

kavscmesrv.rowDATE.log and *store.rowDATE.log* are logs that contain unformatted data. An event will be registered in the *row* log if, for some reason, it could not be entered in the main log.

By default, a new log is created on a monthly basis. The log storage period is not restricted; however, the maximum number of logs having the same format is limited. By default, the application can store not more than 5 logs of the same format. If this maximum allowable is exceeded at the time a new log is created, the oldest log of the same format will be deleted. The frequency for creating new logs and the maximum number of logs can be modified (details see para 11.2, page 111).

New records entered into Kaspersky Anti-Virus logs are added to the end of the newest file. The log size is not restricted.

Kaspersky Anti-Virus logs can be viewed by using the file system.

By default, logs are stored in the **Log** folder. This folder is created in the application's installation folder during the installation of the **Security Server** component. Any other folder selected by the administrator can be used as the log storage (details see para 11.2, page 111).

Kaspersky Anti-Virus logs' settings can be modified in the Diagnostics tab of the application settings window General parameters (see Figure 61). This window is accessible via the [General parameters](#) link.

11.1. Configuring the diagnostics level

The amount and the completeness of the information entered into the logs depend on the diagnostics level for each application module specified in the application settings. If a module consists of several components, the level of diagnostics will be specified for each individual component.

For following diagnostics level are provided:

- **None** – do not log any information.
- **Minimum** – log only major events.
- **Medium** – in addition to major events, log some additional events that describe the Anti-Virus operation in more detail.
- **Maximum** – log full information about the operation of the module, except the debug messages.
- **Debug**– log all information, including debug messages.



In order to configure the diagnostics level,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **Diagnostics** tab in the **General parameters** window that will open (see Figure 61).

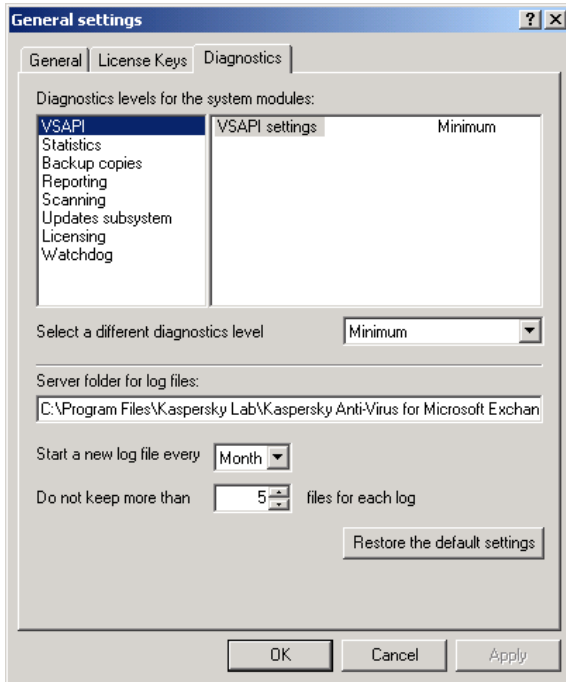


Figure 61. The **Diagnostics** tab

3. The Diagnostics level for system modules section located in the tab contains a table. The left part of the table contains the list of all modules included into the structure of the program. The right part of the table contains the list of components included into the selected module and the diagnostics level for each module.
4. Select the module in the left part of the table and then select the required component in the right part of the table. Select the desired diagnostics level using the Diagnostics level drop-down list.
Specify the required diagnostics level for each module.
5. After you are done with the settings press the **Apply** or the **OK** button.

You can restore the default settings by pressing the **Restore the default settings** button.

11.2. Configuring logs settings



In order to configure logs settings,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **Diagnostics** tab in the **General parameters** window that will open (see Figure 61).
3. Enter the path to the new folder in the **Server folder for log files** field.
4. Select the frequency for creating logs in the **Start a new file every** field by selecting the required value from the drop-down list.
5. Specify the number of log files of the same format that can be stored by the application. In order to do this, specify the desired value in the **Do not keep more than [NN] files for each log** field.
6. After you are done with the settings press the **Apply** or the **OK** button.

You can restore the default settings by pressing the **Restore the default settings** button.

CHAPTER 12. LICENSE KEYS

When you purchase Kaspersky Anti-Virus, you enter a license agreement with Kaspersky Lab Ltd. Based on this agreement, you are granted the right to use the software you purchased during a certain period for the protection of the specified number of mail boxes.



Anti-virus protection covers both mailboxes and public folders. Therefore, you need no additional license for protection of public folders when working in the Microsoft Exchange environment.

The following features will be available for you during the license period:

- using the anti-virus functionality of the application;
- *hourly* anti-virus database updates;
- application updates (patches);
- receiving new versions of the application (upgrades);
- support on issues related to the installation, configuration and the use of the purchased software product, provided 24 hours a day by phone or via email;
- the possibility to send infected and suspicious objects to Kaspersky Lab for expert analysis.

The application verifies the validity of the license agreement by the **license key** that is an integral part of any Kaspersky Lab's product.



Kaspersky Anti-Virus WILL NOT WORK without a license key!

An application can use only one active license key. This license key contains restrictions imposed on the use of Kaspersky Anti-Virus that can be verified by the special application's components. If any violation of the terms and conditions of the license agreement have been detected:

- the functionality of the application will be limited;
- a record about the violation detected will be entered into the events logs;
- if the notification settings are configured, a notification of the violation will be issued and sent by e-mail (details see para 12.3, page 118).



The number of objects not scanned during the period when the application functionality was restricted due to the violation of the license terms, can be viewed in the corresponding section of the **General scan results** report (see para 10.2 on page 104). We recommend that you start a background scan after the anti-virus functionality of the application is restored (after the new license key is installed) to scan these objects.

If the number of protected mail boxes defined in the license is exceeded, the anti-virus functionality of the application will be disabled. In this case, only management services used to configure the application parameters (license key installation and selection of protected storage areas) will be available.

You can change the number of protected mailboxes by excluding some of them from the storage scan scope; such mail boxes will not be scanned (details see para 12.6, page 120).

A preliminary notification about the license restriction on the number of mailboxes is issued when the number of mailboxes on the mail server reaches 90% of the number specified in the license.

We recommend that you purchase additional licenses to ensure anti-virus protection of all mailboxes as any unprotected storage areas increase the possibility of penetration and distribution of viruses via the e-mail system.

Upon the expiration of the commercial license, the functionality of Kaspersky Anti-Virus will be preserved except for the possibility to update the anti-virus database. The application will continue to perform anti-virus traffic scan and background storages scan, but it will use outdated versions of anti-virus database to disinfect objects. In this case, it is difficult to guarantee comprehensive anti-virus protection against new viruses that appeared after the Kaspersky Anti-Virus license expired.

A warning message is displayed when the application is running, two weeks prior to the license expiration date. This message contains information about the expiration date of the currently installed license key.

We recommend that you timely renew your license for using Kaspersky Anti-Virus.



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



In order to renew your license you have to purchase and install a new license key for your Kaspersky Anti-Virus application. In order to do this:

1. Contact the dealer you originally purchased the product from and buy a new license key for the use of Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003.

or

2. Purchase a new license key directly from Kaspersky Labs. In order to do this, send a request directly to the Sales Department of our company (sales@kaspersky.com) or fill in a form at our website (<http://www.kaspersky.com>). Upon the receipt of your payment, we

will send a new license key to the e-mail address specified in your order.

3. Install the license key (see para 12.4, page 119).



You can install two keys: one current key and one backup key. The current key is the active key that you are using. The application cannot use more than one current key. The backup license key will be automatically activated upon the expiry of the current key.

In some cases, as, for example, if the sales contract was terminated or if the license agreement restrictions were changed, Kaspersky Labs terminates the license agreement with the user. In this case the serial number of the license key will be added to the list of cancelled license keys, the so-called "black list".

If your current license key is found in the "black list", the backup key will not be activated and the application functionality will not be available except for the management and the anti-virus database updating services.

12.1. License information



In order to view the license,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **General** tab in the **General settings** window that will open (see Figure 62).

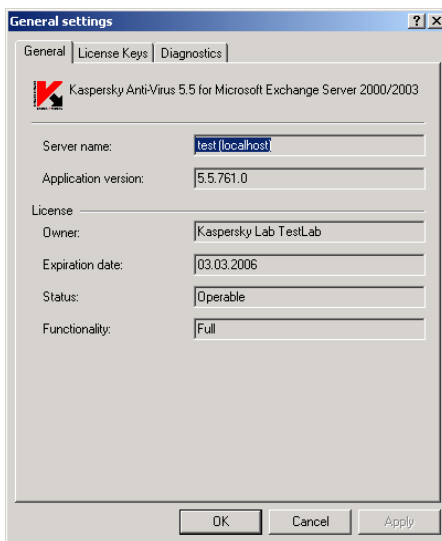


Figure 62. Viewing license information

The tab contains the following information:

- the name of Exchange servers on which the Kaspersky Anti-Virus Security Server component is installed;
- the number of the application version installed;
- License owner information;
- License expiry date;
- the status of the current license key;
- application functionality available based on the current license key:
 - **Full.** The application operates as provided for in the license agreement.
 - **Updates are not available.** The anti-virus database updating feature is not available. The application performs the anti-virus scan and disinfects infected objects found based on the outdated version of the anti-virus database. Your license may be expired.
 - **Management services only.** Only management services used to configure the application parameters (license key installation and selection of protected storage areas) are

available. This may be caused by exceeding the license restriction on the number of protected mailboxes or by the expiration of the trial license key.

- **Update only.** Only anti-virus database updating feature is available. The anti-virus database may have been corrupted; therefore, the anti-virus scan cannot be performed.

12.2. License key details



In order to view information about the license keys installed for the use with the application,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **General** tab in the **General settings** window that will open (see Figure 62).
3. This window contains detailed information about the current and the backup license keys installed and the license-related notifications settings.

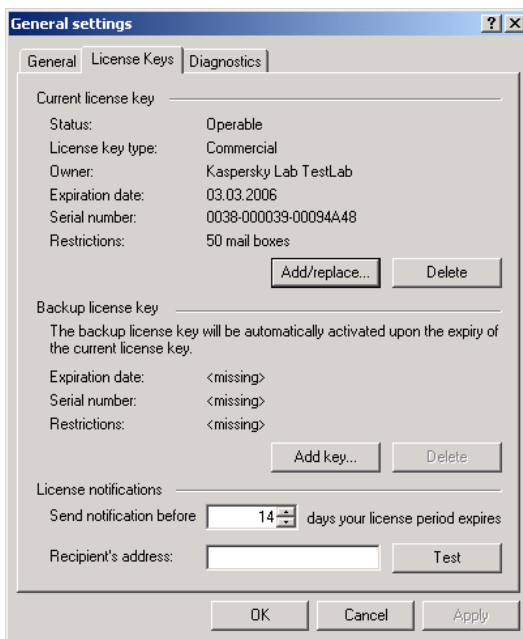


Figure 63. Viewing license key details

The following license key details are displayed in the **Current license key** section.

- Status
- The type of the license key installed, for example: **commercial, trial**.
- License owner information
- License expiration date.
- The maximum number of protected mailboxes.

The following license key details are displayed in the **Backup license key** section.

- License expiration date.
- Serial number
- The maximum number of protected mailboxes.

12.3. License-related notifications

The application verifies the compliance with the terms and conditions of the license agreement on a regular basis and each time the anti-virus database is updated.

If the following is the case based on the verification results:

- the license key expires in several days;
- the license key has expired;
- the current license key was found in the black list;
- The number of mailboxes on the mail server has reached 90% of the maximum number specified in the license;
- The number of mailboxes on the mail server has exceeded the quote specified in the license;

a record will be entered into the application's logs and, if the notification parameters are configured, a message will be sent by e-mail.

By default, a notification will be issued 14 days before your license period is expired. You can set up an earlier or a later notification date.



In order to configure license-related notification,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **License keys** tab in the **General settings** window that will open (see Figure 62).

Enter the following in the **License notifications** sections:

- the number of days before the license expiry date you want the license notification to be issued;
- e-mail address of the recipient of the notifications.

The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.

Entering several e-mail addresses is allowed, the addresses entered must be separated by semicolons.

3. After you have entered and verified the address, press the **Apply** or the **OK** button.

12.4. Installing the license key

Two license keys, the current and the backup key, can be installed for one application. The backup license key automatically becomes the current license key upon the expiry of the current key.



If the current license key is found in the “black list”, the backup key will not be activated. In this case, you have to replace the current license key. You can manually install the backup license key as the current key.

There is a provision for the replacement of the current license key that prevents the restriction of the application functionality if the replacement is performed as the consecutive procedure of the removal of the old current key and installation of the new key.

If no license keys installed for the application, only the current license key can be installed.



In order to install or to replace the current license key,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **License keys** tab in the **General settings** window that will open (see Figure 62).
3. Do the following in the **License keys** tab:
 - if you are installing or replacing the current license key, press the **Add/Replace button** in the **Current license key** section.
 - if you are installing or replacing the backup license key, press the **Add button** in the **Current license key** section.
4. Specify the license key file (*.key) to be installed in the file select dialog box that will open.



After the trial license key is expired you will not be able to install another trial license key

As a result, information about the license key installed will be displayed in the fields of the corresponding section.

5. Close the **General settings** window by pressing the **OK** or the **Apply** button.

12.5. Removing a license key



When you remove the current license key, the backup key will be automatically removed as well.



In order to remove a license key,

1. Select the node corresponding to the required server in the console tree and follow the [General parameters](#) link in the results pane.
2. Go to the **License keys** tab in the **General settings** window that will open (see Figure 62).
3. In the **License keys** tab:
 - if you are removing the backup license key, press the **Remove** button in the **Backup license key** section.
 - if you are removing the current license key, press the **Remove** button in the **Current license key** section.
4. Confirm the removal of the license key in the warning message that will be displayed on your screen.

As a result, information in the fields of the corresponding sections will be updated.

5. Close the **General settings** window by pressing the **OK** or the **Apply** button.

12.6. Unprotected storage areas

The application is designed to ensure protection of the number of mail boxes specified in the license that you purchased. If this number is not sufficient, you will have to decide which mailboxes should be left unprotected and placed into the storage areas not covered by the anti-virus protection.



In order to disable anti-virus protection of a storage area,

1. Select the node corresponding to the required server in the console tree and follow the [Anti-virus protection](#) link in the results pane.
2. Go to the **Protected mail** (see Figure 64) tab in the **Anti-virus protection** window that will open.

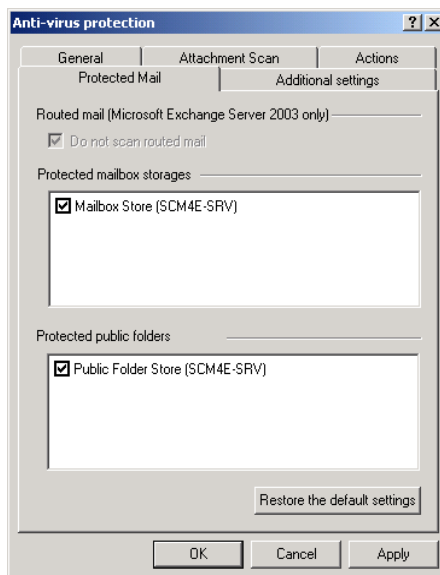


Figure 64. Selecting unprotected storage areas

- Uncheck boxes next to the names of storage areas in the **Protected mailboxes storage areas** section for those storage areas whose mailboxes will not be scanned for viruses.

The list includes all storage areas created on the protected Exchange server. By default, they all will be protected.



E-mail messages sent from, received to or stored in mailboxes within unprotected storage areas, will not be scanned for viruses.

- Uncheck boxes next to the names of public folders in the **Protected public folders storage areas** section for those storage areas the content of which will not be scanned for viruses.

The list includes all storage areas of public folders created on the protected Exchange server. By default, they all will be protected.

3. In order to apply the changes, press the **Apply** or the **OK** button.

You can restore the default settings by pressing the **Restore the default settings** button.

As a result, the mailboxes located in the unprotected storage areas will not be counted when the verification of the compliance with the license restrictions is performed.

CHAPTER 13. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to questions most frequently asked by users regarding the installation, setup, and operation of Kaspersky Anti-Virus. We will try to answer them here in detail.



Question: Can Kaspersky Anti-Virus be used with other vendors' anti-virus software?

In order to avoid conflicts we recommend that you remove any third-party anti-virus software before you install Kaspersky Anti-Virus.



Question: Why do I need a license key? Will my Anti-Virus work without it?

Kaspersky Anti-Virus will not work without a license key.

If you are still undecided whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will only work either for two weeks or for a month. When this period expires, the key will be blocked.



Question: What happens when my Kaspersky Anti-Virus license expires?

After the expiration of the license, Kaspersky Anti-Virus will continue operating, but anti-virus database updating feature will be disabled. The anti-virus application will continue disinfecting objects infected with viruses but it will be using old anti-virus database.

When this happens, inform your system administrator or contact the dealer you purchased your copy of Kaspersky Anti-Virus from or Kaspersky Lab directly.



Question: My Anti-Virus does not work. What should I do?

First of all, try to find your problem description and its solution in this document (particularly this section) or in our website.

We also recommend that you contact the dealer you purchased your copy of Kaspersky Anti-Virus from or send an e-mail message to our Technical support service (support@kaspersky.com) or at the address specified in your license key details.

To ensure that your request is answered as soon as possible, follow the below suggestions:

1. In the subject of your message, indicate your operating system, the name of the Kaspersky Lab's product you are using and the problem you have encountered. For example, **Microsoft Windows 2000, Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003, cannot update anti-virus database.**
2. Use plain text format for your messages.
3. At the beginning of your message, indicate:
 - the version of your operating system and service packs installed;
 - the version of your Microsoft Exchange Server and service packs installed;
 - the version of your Kaspersky Anti-Virus copy and the number of your license.
4. Briefly, but clearly describe the problem. Bear in mind that the support specialists have no previous knowledge of your problem and can only help you if they fully understand it and have been able to reproduce it.
5. Forward to the technical support service the following data packed in one archive:
 - the current application events logs produced with the **Debug** diagnostic level for each module;
 - The license key.
6. Make sure that you have specified the following conditions in your message:
 - RAM less than 256 MB or more than 2 GB.
7. Indicate the approximate daily traffic and load peaks if applicable.



Question: Why daily updates are required?

Several years ago viruses distributed via floppy disks and at that time it was sufficient for computer protection to install an anti-virus program and update the anti-virus database from time to time. Yet, the recent virus outbreaks spread over the world in a matter of several hours and anti-virus software using old anti-virus database may not be able to protect you against a new threat. Therefore, to ensure protection against new viruses you have to update your anti-virus database on a daily basis.

Kaspersky Lab shortens the update interval for the anti-virus database located at the server each year. Now the anti-virus database is updated at the server every hour.

An additional feature available is the updating of the Anti-Virus application modules to repair detected vulnerabilities or offer new functionality.



Question: I use a proxy server and cannot perform updates. What should I do?

Failure to receive updates via a proxy server can be attributed to the following:

- Incorrect network settings.

When configuring the update service you can specify the network settings using one of the two below methods: using your Microsoft Internet Explorer settings or using custom settings. In certain cases detailed below, the update service may use the Microsoft Internet Explorer settings incorrectly:

- internet settings are not configured on your computer;
- Microsoft Internet Explorer settings are not available if no users are logged in;
- your proxy server requires authorization.

In these cases the network settings should be configured in the update service settings.

- your proxy server is not supported by the Kaspersky Anti-Virus update service.

Kaspersky Anti-Virus update service is not compatible with Kerio WinRoute proxy server as WinRoute does not fully support the http 1.0 protocol. In this case we recommend using a different proxy server.

APPENDIX A. TABLE OF SUBSTITUTION MACROS

Macros	Macros meaning
%%	
%OCURRENCE_NUMBER%	The total number of registered events
%PERIOD_LENGTH%	period length
%PERIOD_TYPE%	unit used to specify the time period (seconds, minutes, hours, days)
%VIRUS_NAME%	the name of the detected virus (in virus outbreaks notifications used only for the One and the same virus detected several times event)
%ACTION%	action performed with the object during the anti-virus scan
%AVBASES_LAST_UPDATE%	last anti-virus database update date
%CC%	the list of the recipients of the message carbon copy (cc)
%CONTENT_CODEPAGE%	message object content codepage
%CONTENT_LENGTH%	object size
%CONTENT_TYPE%	MIME object information
%DATABASE_NAME%	the name of the Microsoft Exchange Server 2000 database where the object was detected
%FROM%	Displayed sender's name
%MAILBOX_NAME%	name of the mailbox in which the object was detected
%MESSAGE_URL_NAME%	full name of the message where the object was detected

Macros	Macros meaning
%OBJECT_NAME%	attachment name, not defined for OLE objects and for messages
%OBJECT_TYPE%	object type: message, file, OLE object
%RECV_TIME%	time the message was received
%SCANNER_VERSION%	application version number
%SCANNER_VENDOR%	application vendor name - Kaspersky Lab
%SENT_REPRESENTING_NAME%	displayed name of the message exchange user provided by the sender
%SERVER_NAME%	name of the server on which the object was detected (when the application is working on the servers cluster - the name of a virtual server; in the virus outbreak notifications – the name of the cluster node).
%SUBJECT%	message subject
%SUBMIT_TIME%	time the message was sent
%TO%	list of message recipient

APPENDIX B. GLOSSARY

The product's documentation contains terms and concepts specific to the field of anti-virus protection. This glossary contains definitions of such concepts. For your convenience, the terms are arranged in the alphabetic order.

A

Administrator's workstation – a computer on which the Management Console (a component of Kaspersky Anti-Virus) is installed. This computer is used to configure and manage the server part of the application called the Security Server.

Anti-virus database – database, created by Kaspersky Lab's specialists, containing detailed descriptions of all currently existing viruses and methods for their detection and disinfection. Our anti-virus database is constantly updated by Kaspersky Lab as new viruses appear. Therefore, the administrator must update the anti-virus database, used by the application, on a regular basis.

B

Background scan – anti-virus scan of e-mail messages stored on the server and of the content of the public folders using the latest version of the anti-virus database. This scan involves public folders and protected storages (mailbox storage). The scan may identify new viruses that were not described in the anti-virus database at the time when previous scans were performed.

Backup copying – creation of a backup copy of an object before it is processed and moving this copy into a backup storage. Object stored in the backup storage can later be restored, sent to Kaspersky Lab for analysis or deleted.

Backup license key – a license key installed for Kaspersky Anti-Virus but not yet activated. The backup key starts functioning when the license provided by the current key expires.

Backup storage (BACKUP) is a special storage area for storing backup copies of objects before these objects are disinfected, deleted or replaced. It is a service folder created in the application's installation folder during the installation of the Security Server component.

Black list – a database that contains information about license keys whose owners infringed the terms of the License Agreement and about keys that have been created but, for any reason, have not been sold. The content of the black list is updated on a daily basis.

C

Container object – an object subject to anti-virus scan that consists of several objects, such as an archive, a message containing an attached message, etc. See also **simple object**.

D

Deleting the object – a method of object processing that involves physical removal of object from the computer. We recommend using this method for processing infected objects. If deletion is the primary action assigned to the object, a backup copy of such object will be created before this action is performed.. You can use this copy later to restore the original object.

Disinfection – a method used for processing infected objects that results in full or partial restoration of data or a decision that the object cannot be disinfected. Disinfection is performed based on the records contained in the *anti-virus database*. If disinfection is the primary action assigned to the object (i.e. if it is the first action to be performed on an object after it is detected), a *backup copy* of such object will be created before this action is performed. Part of the data may be lost during the process of disinfection. A backup copy of the object can be used to restore the object in its original state.

I

Infected object – an object containing malicious code. We do not recommend accessing these objects because this may result in an infection of your computer.

K

Kaspersky Administration Kit – an application included into Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite and designed to provide a centralized solution for most important administration tasks associated with managing the corporate network anti-virus security system based on Kaspersky Lab's applications.

Kaspersky Lab's updating servers – a list of http- and ftp sites of Kaspersky Lab from which Kaspersky Anti-Virus downloads anti-virus database and application modules updates.

L

License key – a file with *.key extension that is your personal key required to use Kaspersky Anti-Virus. The license key is included into the product's distribution kit if you purchased it from a Kaspersky Lab's dealer or will be e-mailed to you if you purchased the product online. Kaspersky Anti-Virus WILL NOT WORK without a license key!

License period– a period of time during for which you are granted the right to use all features of Kaspersky Anti-Virus. The license period is determined by the license key; a standard license period is one year after the

license key is installed. After the license expires, the application functionality will be restricted.

M

Management console – a component of Kaspersky Anti-Virus. Management Console provides the user interface for managing the administration services of the application and for configuring settings and managing the server component. The management module is implemented as the Microsoft Management Console (MMC) extension.

N

Notification template – a template used to create notifications about infected objects detected during the anti-virus scan. A notification template contains a set of parameters that define the notification procedure, the distribution method and the text of notifications to be sent.

R

Replacement template – a template used to create a text notification about infected objects detected or about a threat of a virus outbreak.

Report template – a template used to create reports on the results of the anti-virus server scan. A report template contains a set of parameters that define the reporting period, the reporting schedule and the report format.

Restoring – a process that involves moving of the backup copy of an object from the backup storage into a folder specified by the administrator, decoding and saving with a specified name. The restored file will have the same format as it had before it was first processed by Kaspersky Anti-Virus.

S

Security Server – a server component of the Kaspersky Anti-Virus application. Security Server provides the anti-virus functionality and updating of the anti-virus database and includes administration services for remote management, configuring and ensuring the integrity of the application and of the data stored.

Simple object – an object subject to anti-virus scan: a message body or a simple attachment, as, for example, an executable file. See also: **Container object**.

Storage scan – see **Background scan**.

Suspicious object – an object that contain modified code of a known virus or code that resembles code of a virus, but not known by Kaspersky Lab at the moment.

T

Traffic scan – anti-virus scan of e-mail messages received by the Exchange server in the real-time mode using the current (latest) version of the anti-virus database.

U

Unknown virus – a new virus the *anti-virus database* contain no information about. As a rule, Kaspersky Anti-Virus detects unknown viruses contained in objects using *heuristic code analyzer* and such objects are assigned the *suspicious* status.

Updating of anti-virus database – a process of replacement of or appending new records to the anti-virus database received by the application from the Kaspersky Lab's updating servers or from a network folder.

V

Virus activity level threshold – a maximum allowable number of events of a certain type within a specified time interval; when this number is exceeded, the situation is classified as increased virus activity and a threat of virus attack. This value is of great significance in the periods of virus outbreaks as it helps the administrator timely react on the emerging threats of virus attacks.

Virus outbreak counter – a template used to create and issue notifications about a virus outbreak threat. The virus outbreak counter contains a set of parameters that determine the virus activity level threshold, the distribution method and the text of notifications to be sent.

APPENDIX C. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted 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 and Poland. 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 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls and Internet-gateways, 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 3 hours. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

C.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus Personal protects home computers running Windows 98/ME/2000/NT/XP from all types of known viruses, including Riskware. The application constantly monitors all possible sources of virus penetration, including email, Internet, floppy disks, and CDs. Unknown viruses are efficiently detected and processed by a unique heuristic data analysis system. The two distinct modes of the application's operation (that can be used either separately or jointly) are:

- **Real-Time Protection** – anti-virus scan of all files being run, opened or saved on the protected computer.
- **On-Demand Scan** – scanning and disinfection of the entire computer or individual disks, files or folders. You can launch such a scan manually using the graphical interface, or schedule a regular automated scan.

Kaspersky Anti-Virus Personal does not scan objects which have not been modified since their previous scan. This rule now applies both to real-time protection and to the on-demand scan. This feature **greatly improves the speed and performance of the program**.

Kaspersky Anti-Virus Personal provides reliable protection against viruses that attempt to penetrate computers via email messages. The application automatically scans and disinfects all incoming (POP3) and outgoing (SMTP) email messages and efficiently detects viruses in email databases.

Kaspersky Anti-Virus Personal supports over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content, and removal of malicious code from files within **ZIP, CAB, RAR** and **ARJ** archives.

The application's settings can easily be adjusted by selecting one of three pre-defined levels: **Maximum Protection**, **Recommended Protection** and **Maximum Speed**.

The anti-virus database is updated every three hours. Database delivery is guaranteed even if the internet connection is interrupted or switched during the download process.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Windows 98/ME/2000/NT/XP as well as Microsoft Office 2000 applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A second-generation heuristic analyzer efficiently detects unknown viruses. Kaspersky Anti-Virus Personal includes many interface enhancements, making it easier than ever to use the program.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks;
- **Real-time automatic protection** of all accessed files from viruses;
- **Mail filter** automatically scans and disinfects all incoming and outgoing mail traffic (POP3 and SMTP) and effectively detects viruses in mail databases;
- **Behavior blocker** that provides maximum protection of Microsoft Office applications from viruses;
- **Archive scans** – Kaspersky Anti-Virus recognizes over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR** and **ARJ** archives.

Kaspersky® Anti-Hacker

Kaspersky Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, it prevents the suspicious application from accessing the network. This enhances your privacy and provides 100% security for confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

- Kaspersky Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.
- Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes the firewall adjustable to your specific preferences and your particular needs.

Kaspersky® Security for PDA

Kaspersky Security for PDA provides reliable anti-virus protection of data stored on PDAs running Palm OS or Windows CE. It also offers anti-virus protection from corrupted files transferred from a PC or an extension card, from ROM files, or from databases. This software package includes an optimal combination of the following anti-virus tools:

- **anti-virus scanner** to scan the data stored on both the PDA and extension card on demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus Business Optimal includes full-scale anti-virus protection¹ for:

- *Workstations* running Windows 98/ME/NT/2000/XP Workstation, and Linux;
- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, and Linux;
- *Email clients*, namely Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail;
- *Internet-gateways*: CheckPoint Firewall –1; Microsoft ISA Server.

The Kaspersky Anti-Virus Business Optimal distribution kit includes Kaspersky Administration Kit, a *unique tool for automated deployment and administration*.

All of these components are interoperable so that any of them can be selected, 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 Windows 98/ME/NT/2000/XP, and Linux;

¹ Depending on the type of distribution kit.

- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD and Linux;
- *Email clients*, including Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet-gateways*: CheckPoint Firewall –1; Microsoft ISA Server;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS.

The Kaspersky Corporate Suite distribution kit includes Kaspersky Administration Kit, a *unique tool for automated deployment and administration*.

All of these components are fully interoperable so that any of them can be chosen, 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 all modern methods of email filtration (including RBL 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, Kaspersky Anti-Spam monitors incoming email and acts as a barrier to unsolicited email. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky Anti-Spam's high performance is ensured by daily updating of the content filtration database with samples provided by Kaspersky Lab's linguistic laboratory.

Kaspersky® Anti-Spam Personal

Kaspersky Anti-Spam Personal is designed to protect users of mail client programs Microsoft Outlook and Microsoft Outlook Express against unwanted email messages (spam).

Kaspersky Anti-Spam Personal software package is a powerful tool that detects spam in incoming email messages received via the POP3 or IMAP4 protocols (only for Microsoft Outlook).

The filtering process involves the analysis of all attributes of the letter (sender's and recipient's addresses and headers), content filtration (analysis of the content of the letter, both the subject and any attached files), using unique linguistic and heuristic algorithms.

The application's performance is enhanced by daily updating of the content filtration database with samples provided by Kaspersky Lab's linguistic laboratory.

C.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. All of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com

APPENDIX D. LICENSE AGREEMENT

End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD'S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) PURCHASED ON LINE FROM THE KASPERSKY LAB INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF 7 WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You

may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on ww.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means:

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Limitation of Liability.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

- (d) Loss of anticipated savings;
- (e) Loss of business;
- (f) Loss of opportunity;
- (g) Loss of goodwill;
- (h) Loss of reputation;
- (i) Loss of, damage to or corruption of data, or:
- (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii) below, you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).