

KASPERSKY LAB  
Kaspersky Security<sup>®</sup> 5.5  
for Microsoft Exchange Server  
2003

ADMINISTRATOR'S  
GUIDE

KASPERSKY SECURITY 5.5  
FOR MICROSOFT EXCHANGE SERVER 2003

---

# Administrator's Guide

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

Revision date: November 2006

# Table of Contents

CHAPTER 1. INTRODUCTION .....	7
1.1. Threats to the computer security .....	7
1.2. The purpose and major functionality of the application .....	10
1.3. Hardware system requirements .....	12
1.4. Software system requirements .....	12
1.5. Distribution kit .....	12
1.6. Services provided for registered users .....	13
1.7. Conventions .....	14
CHAPTER 2. OPERATION OF THE APPLICATION .....	15
2.1. Security Server architecture .....	16
2.2. Server protection deployment .....	17
2.3. Server protection system maintenance .....	18
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 .....	24
3.2. Removing the application .....	25
3.3. Upgrading from a previous version .....	25
CHAPTER 4. STARTING USING THE APPLICATION .....	26
4.1. Starting the application .....	26
4.2. Application interface .....	26
4.2.1. Main application window .....	26
4.2.2. Shortcut menu .....	28
4.3. Creating the list of managed servers .....	30
4.4. Connecting the Management Console to the server .....	31
4.5. Minimum required configuration .....	32
4.6. Mail server protection without additional configuration .....	33
4.7. Verifying the application performance .....	35

---

4.7.1. Testing the anti-virus protection system .....	35
4.7.2. Testing the anti-spam protection system .....	36
CHAPTER 5. UPDATING THE ANTI-VIRUS AND THE CONTENT FILTRATION DATABASES .....	38
5.1. Manual updating .....	39
5.2. Automatic updates .....	40
5.3. Selecting the updates source .....	41
5.4. Configuring the connection settings .....	43
5.5. Running updates under a different user account .....	45
CHAPTER 6. ANTI-VIRUS PROTECTION .....	47
6.1. Anti-virus protection levels .....	49
6.2. Enabling and disabling the anti-virus server protection. Selecting anti-virus protection level .....	51
6.3. Scanning attachments .....	53
6.4. Scanning of routed e-mail traffic .....	56
6.5. Selecting actions to be performed with objects .....	57
6.6. Background scan .....	62
CHAPTER 7. ANTI-SPAM PROTECTION .....	65
7.1. Enabling/disabling anti-spam protection .....	66
7.2. Selecting the action to be performed with the message .....	67
7.3. Configuring TCP/IP settings .....	70
7.4. Configuring e-mail filtration .....	70
CHAPTER 8. APPLICATION'S OPERATION EFFICIENCY .....	72
8.1. Anti-virus protection efficiency .....	72
8.2. Anti-spam protection efficiency .....	73
CHAPTER 9. BACKUP COPYING .....	74
9.1. Viewing backup storage .....	75
9.2. Backup storage filter .....	77
9.3. Restoring objects from the backup storage .....	80
9.4. Sending e-mails to addressees .....	81
9.5. Sending objects for analysis .....	81
9.6. Deleting objects from the backup storage .....	82
9.7. Configuring the backup storage settings .....	83

---

CHAPTER 10. NOTIFICATIONS .....	86
10.1. Creating a notification template.....	87
10.2. Viewing and editing notification parameters.....	91
10.3. Customizing general notification settings .....	91
CHAPTER 11. PREVENTING VIRUS OUTBREAKS.....	93
11.1. Creating a new virus outbreak counter.....	95
11.2. Viewing and modifying virus outbreak notification settings.....	99
CHAPTER 12. REPORTS.....	100
12.1. Receiving reports.....	102
12.1.1. Creating a report template.....	104
12.1.2. Viewing and fine-tuning the report templates .....	107
12.2. Viewing reports.....	108
CHAPTER 13. APPLICATION'S EVENT LOGS.....	111
13.1. Configuring the diagnostics level .....	112
13.2. Configuring log settings.....	114
CHAPTER 14. LICENSE KEYS.....	115
14.1. License information .....	117
14.2. Installing the license key .....	119
14.3. Removing a license key.....	121
14.4. License-related notifications.....	121
14.5. Unprotected storage areas .....	122
CHAPTER 15. APPLICATION MANAGEMENT USING KASPERSKY ADMINISTRATION KIT.....	124
15.1. Managing policies.....	126
15.1.1. Creating a policy .....	126
15.1.2. Viewing and editing policy settings .....	130
15.1.2.1. Viewing information about the application .....	131
15.1.2.2. Enabling / disabling server protection .....	132
15.1.2.3. Scanning of attachments.....	133
15.1.2.4. Scanning of routed mail.....	134
15.1.2.5. The choice of actions over objects.....	135
15.1.2.6. The choice of actions over spam messages .....	136
15.1.2.7. Configuring the server protection productivity.....	137
15.1.2.8. Updating the anti-virus and content filtration databases.....	138

---

15.1.2.9. Notifications on detected objects.....	139
15.1.2.10. Virus outbreak notification .....	140
15.1.2.11. General notification settings .....	140
15.1.2.12. Additional settings.....	141
15.1.2.13. Registration of events on program operation on Administration Server.....	142
15.1.2.14. Reviewing the results of policy application .....	144
15.2. Management of application settings .....	145
15.2.1. Reviewing the information about application .....	147
15.2.2. Reviewing the license key information.....	148
15.2.3. Start background scan .....	148
15.2.4. Selection of protected storage .....	149
15.2.5. Viewing reports .....	150
15.3. Task management .....	152
15.3.1. Running and stopping tasks.....	154
15.3.2. Configuring task parameters .....	155
CHAPTER 16. FREQUENTLY ASKED QUESTIONS.....	156
APPENDIX A. TABLE OF SUBSTITUTION MACROS .....	160
APPENDIX B. CONTACTING THE TECHNICAL SUPPORT SERVICE .....	163
APPENDIX C. GLOSSARY .....	165
APPENDIX D. KASPERSKY LAB.....	170
D.1. Other Kaspersky Lab Products .....	171
D.2. Contact Us .....	179
APPENDIX E. LICENSE AGREEMENT.....	180

---

# CHAPTER 1. INTRODUCTION

The main source of viruses today is the global Internet. Most virus infections happen via 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 (SPAM) and misuse of the Internet resources. Although not a direct threat, unsolicited e-mail messages increase the load on the mail servers, fill mailboxes with unwanted messages, 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 information has become an important asset. 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. Threats to the computer security**

There are a vast number of threats that could affect your computer today. Reading this chapter will give you a general understanding of them.

### **Worms**

This malicious program category largely exploits operating system vulnerabilities to spread itself. The class was named for the way the worms

crawl from computer to computer, using networks, e-mail, and other data channels. This feature gives many worms a rather high speed in spreading themselves.

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

## Viruses

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

## Trojans

Programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang, stealing confidential information, etc. These malicious programs are not viruses in the traditional sense of the term, since they do not infect other programs or data; Trojans are not capable of independently penetrating computers. Their users spread them under the guise of useful software. The damage that they incur can exceed that done by traditional virus attacks by several fold.

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.



Henceforth in the text of this Administrator's Guide the term "virus" will be used to refer collectively to viruses, Trojan Horses, and worms. A particular type of malware will be mentioned only when it is required.

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

## Adware

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

## **Riskware**

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

## **Spyware**

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

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

## **Jokes**

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

## **PornWare**

Programs that make modem connections with various pay-per-use websites, generally pornographic in nature.

## **Hack Tools**

Software used by hackers to penetrate your computer for their own ends. They include various illegal vulnerability scanners, password cracking programs, and other types of programs for cracking network resources or penetrating a system.

## **Other dangerous programs**

Programs created to set up DoS attacks on remote servers, hacking into other computers, and programs that are part of the development environment for malicious programs. These programs include hack tools, virus

builders, vulnerability scanners, password cracking programs, and other types of programs for cracking network resources or penetrating a system.

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.

Another threat that e-mail users face daily is spam. **Spam** is anonymous junk e-mail. Spam includes mailings that are marketing, political and provocative in nature and e-mails asking for assistance. Another category of spam includes e-mails that ask one to invest large amounts of money or to get involve in pyramid schemes, e-mails aimed at stealing passwords and credit card numbers, and e-mails that ask to be sent to friends (chain letters), etc. Spam significantly increases the load on mail services and increases the risk of losing information that is important for the user. Spam can be roughly divided into four categories:

- **Formal messages** – messages that are automatically generated and sent to recipients by automated mail program functions (as, for example, notifications of undeliverable messages or confirmation of the user's registration at some Internet website);
- **Probable SPAM** - messages that can not be unambiguously identified as SPAM, but that raise suspicions when checked (for example, some types of mass mailing and advertising messages);
- **Obscene messages**– messages that contain obscene language;
- **SPAM messages** – message that definitely contain SPAM.

## 1.2. The purpose and major functionality of the application

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 (hereinafter referred to as **Kaspersky Security**) is designed to ensure protection of mailboxes and public folders located on Microsoft Exchange Server 2003 (hereinafter **Microsoft Exchange Server**) against malicious programs and unsolicited e-mail messages (SPAM).

Kaspersky Security performs the following functions:

- *scanning and analyzing incoming and outgoing e-mail messages* for the presence of malicious objects. This analysis processes the bodies and attachments of e-mail messages. Depending on the settings configured, the application will disinfect or delete a malicious object or will add a warning message to such objects;

- *scanning e-mail messages received by the Exchange server via SMTP protocol for SPAM* including the analysis of all attributes and attachments of the message. Depending on the settings, the application will deliver the message to the **Inbox** folder, move the message to the **Junk E-mail** folder, block the message or delete it. In addition to the first two actions, special markers can be added to the subject line of the message;
- *saving backup copies of the message's objects* before an attempt to disinfect or delete such object (during an anti-virus scan) and copies of messages before they are blocked or deleted (during an anti-spam scan); 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 messages that contain malicious objects or may contain SPAM.
- *maintaining the event log and creating regular reports* about the operation of the application, the status of the anti-virus protection and anti-spam protection. The application allows generation of reports using templates with a preset level of detail and at a 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.);
- *updating the anti-virus database and content filtration database* automatically or manually. The databases can be updated from the Kaspersky Lab's FTP and HTTP web servers or from a local/network folder that contains the latest set of updates;
- *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 mailboxes;
- *managing license keys.*

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 includes the following components:

- **Security Server** performs the scan of the mail traffic for viruses and spam, updates the anti-virus database and content filtration database, provides 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 enables you to configure settings and manage the server component. The management module is implemented as the extension of the Microsoft Management Console.

## 1.3. Hardware system requirements

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

## 1.4. Software system requirements

### Requirements to protected server:

- 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 / Microsoft Windows Server 2003 Standard Edition and higher / Microsoft Windows Server 2003 Enterprise Edition and higher;
- Microsoft Exchange Server 2003 Enterprise Edition / Standard Edition.

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

- Microsoft Windows 2000 with Service Pack 4 installed or higher / Microsoft Windows XP / Microsoft Windows 2003;
- Microsoft Management Console (MMC) version 1.2 or higher.

## 1.5. Distribution kit

You can purchase the product from our dealers (retail box) or online (for example, you may visit [www.kaspersky.com](http://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 Security 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. that contains the terms and conditions on which you may use the anti-virus product that 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 the software product 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.

## 1.6. Services provided for registered users

Kaspersky Lab Ltd. offers to all legally registered users an extensive service package enabling them to boost the performance of Kaspersky Security 5.5 for Microsoft Exchange Server 2003.

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.

## 1.7. Conventions

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

Format feature	Meaning/Usage
<b>Bold font</b>	Titles of menus, menu items, windows, dialog boxes and their elements, etc.
 <b>Note.</b>	Additional information, notes
 <b>Attention!</b>	Information requiring special attention
 <i>In order to perform...</i>  1. Step 1. 2. ...	Description of the successive user's steps and possible actions
 Task, example	Statement of a problem, example of the demonstration of the application's capabilities
<b>[key]</b> – modifier name	Command line modifier
Information messages and command line text	Text of configuration files, information messages and command line

---

# CHAPTER 2. OPERATION OF THE APPLICATION

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 scans and, if it is possible, disinfects all incoming and 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.

Additionally, Kaspersky Security performs an anti-spam scan of all messages received by Exchange server via SMTP protocol.

The detection of malicious programs, disinfection of infected objects and detection of messages that contain any type of SPAM is performed based on the records contained in the anti-virus and the content filtration databases. These databases are updated by Kaspersky Lab on a regular basis and the updated versions are uploaded to the Kaspersky Lab's website. Additionally, the application uses a special analysis facility called a heuristic analyzer that allows detecting new viruses that are not even known at the moment.

The application scans objects received by the server in the real-time format. The user cannot open and view a new message before it is scanned.

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 in the background mode 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 database, such message will be re-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 database, no matter when a particular message arrived to the server.

The application processes each object applying actions specified by the administrator to objects of a particular type. For instance, an infected object can be disinfecting, deleted or replaced with a notification. The administrator may select a mode in which the application will deliver messages with infected objects to the user, although it will change the object's name (by adding information about the virus) and the object's extension.

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

The application sends notifications about events occurred to the administrator, the recipient and the sender of the infected message and also places a record about this event into the Kaspersky Security application log file and into the Microsoft Windows event log.

If the virus outbreaks detection facility is enabled, the application will register the virus activity level and will send a notification about the virus outbreak threat or place a corresponding record into the Microsoft Windows event log and into the Kaspersky Security application log file.

## 2.1. Security Server architecture

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

- **E-mail VSAPI Interceptor** 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 2.5 technology.
- **SMTP E-mail Interceptor** intercepts objects arriving to Microsoft Exchange Server via SMTP protocol and forwards them to the anti-spam scan subsystem.
- **Anti-spam Scan Subsystem** scans e-mail messages for spam. This feature is implemented as a Microsoft Windows service, which starts automatically when a message that must be scanned arrives.
- **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 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 any anti-virus applications installed in the corporate network.
- The **Internal Application Management and Integrity Control Module** is launched in a separate process and is a 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. Server protection deployment



*In order to create the system of mail servers protection against malicious programs and SPAM using Kaspersky Security 5.5 for Microsoft Exchange Server 2003:*

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 together, 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 section 4.6, page 33).

The server protection against malicious programs and SPAM will be enabled automatically when Microsoft Exchange Server is started.

3. Create the list of managed servers (see section 4.3, page 30)
4. Connect the Management Console to the servers (see section 4.4, page 31).
5. Configure the protection system for each server:
  - Configure the anti-virus database and content filtration database updating settings (details see Chapter 5, page 38).
  - Verify the correctness of the settings and of the application's operation
    - using a test "virus" **EICAR** (see section 4.7.1, page 35).
    - using a test message that contains spam attributes (see section 4.7.2, page 36).
  - Configure the notification system that issues notifications about events registered during the application's operation (see Chapter 10, page 86)
  - Configure the event logs and reports (Chapter 12, page 100, Chapter 13, page 111).

- Configure the settings for detecting virus outbreaks and notification about such events. (Chapter 11, page 93).

## **2.3. Server protection system maintenance**

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

- periodic updating of the anti-virus and the content filtration databases;
- receiving and processing notifications about detection of objects containing malware or SPAM and about threats of virus outbreaks;
- regular review of reports about the application operation and about the state of the mail server protection;
- processing and cleaning of the backup storage.

## **2.4. Application's operation on a cluster of servers**

Kaspersky Security 5.5 for Microsoft Exchange Server 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. The application will process a message at the node to which this message had been forwarded by the virtual Exchange server.

The scan results for each node of the cluster, namely,

- backup storage contents;
- information included into the reports;
- the group of events registered in the Microsoft Windows event log and in the application's log files;
- 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 protection of Microsoft Exchange Server, installed on the cluster, against malware and SPAM:*

1. Install the **Security Server** component on 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 section 4.3, page 30).

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 Console to the servers (see section 4.4, page 31).
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 section 9.7, page 83).
  - 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 section 12.1.2, page 107 and section 13.2, page 114).
  - The list of unprotected storage areas on all servers must match (see section 14.5, page 122).

---

# CHAPTER 3. INSTALLING, UPDATING AND REMOVING THE APPLICATION

Before starting installation of the application, make sure that the software and hardware of your computer meet the installation requirements (details see section 1.4, page 12).



In order to install, update the version or remove Kaspersky Security 5.5 for Microsoft Exchange Server 2003 from your computer, you will need administrator privileges on the domain.

## 3.1. Installing the application

The installer is a Microsoft Windows setup wizard, which will guide you through several dialogs (steps), which can be navigated using the **Back** and **Next** buttons. The setup wizard will complete its work after clicking the **Finish** button. The **Cancel** button can be used at any moment to exit the wizard.

The wizard will offer you to install the application components of Kaspersky Security 5.5 for Microsoft Exchange Server 2003 (Security Server and Management Console). 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 Security.

After the Management Console is installed, a group **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** and an application icon will appear in **Run/Programs** 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 Security 5.5 for Microsoft Exchange Server 2003;
- startup type – **automatic**;
- account – **Local system**.

The properties of the **Security Server** can be viewed and its operation can be monitored using standard Microsoft Windows administration tools - **Computer Management/Services**. Information about the operation of the **Security Server**

is registered and saved in the Microsoft Windows event log on the computer on which the Security Server is installed.

### 3.1.1. First-time installation

In order to install Kaspersky Security into your computer run the executable 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 of Kaspersky Security 5.5 for Microsoft Exchange Server 2003.

If Microsoft Exchange Server is not installed on your computer or if its version does not meet the software requirements, a warning will be displayed on your screen. In this case, you can proceed with the installation, but you will only be able to use one of the application components – the Management Console.

In order to install the full version of Kaspersky Security, abort the installation process, install or update your software as per the software requirements and reinstall Kaspersky Security.

#### Step 2. Searching for other anti-virus software

This step involves searching for other installed anti-virus products for Microsoft Exchange Server, which may conflict with Kaspersky Security.

- 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 to proceed with the installation of Kaspersky Security, agree to remove the incorrect registration.
- If other vendors' anti-virus software for Microsoft Exchange server is detected installed on your computer, a message will be displayed with a recommendation to remove such existing application before installing

Kaspersky Security. Remove the existing program and then run the installer of Kaspersky Security again.

- If the setup detects that Kaspersky Security 5.5 for Microsoft Exchange Server 2003 (release version, MP1) is installed on the computer, it will suggest upgrading the application to Kaspersky Security 5.5 for Microsoft Exchange Server 2003 MP2 (see section 3.3, page 25).
- If the setup detects that Kaspersky Anti-Virus for Microsoft Exchange is installed, it will display a warning. Then you will have to remove the earlier version of Kaspersky Anti-Virus to install Kaspersky Security. Then run again the installer from the distribution package of Kaspersky Security.

### Step 3. Greeting and License Agreement

As soon as the installer completes checking conformity of software requirements and searching for installed anti-virus applications, it will display a greeting window and a window containing the License Agreement.

Read the text of the License Agreement and accept the terms and conditions contained therein to proceed with the installation.

### Step 4. Selecting the type of the installation

In the dialog for setup type selection, specify whether both application components (Security Server and Management Console) should be installed (*complete installation*) or just one of them (*custom installation*).

If you run installation from the Exchange server that needs to be protected and you plan to manage the application from this computer, select the complete installation option. The application will be installed into the default folder (**...\Program files\Kaspersky Lab\Kaspersky Security 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.

### Step 5. Selecting application components to be installed

If you selected the custom installation at the previous step, you will have to specify which application components must be installed on your computer in the dialog box shown on Figure 1. You can also change the default destination folder.

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 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 Security for Microsoft Exchange Server** folder. You can change the default installation folder using the **Browse** button.

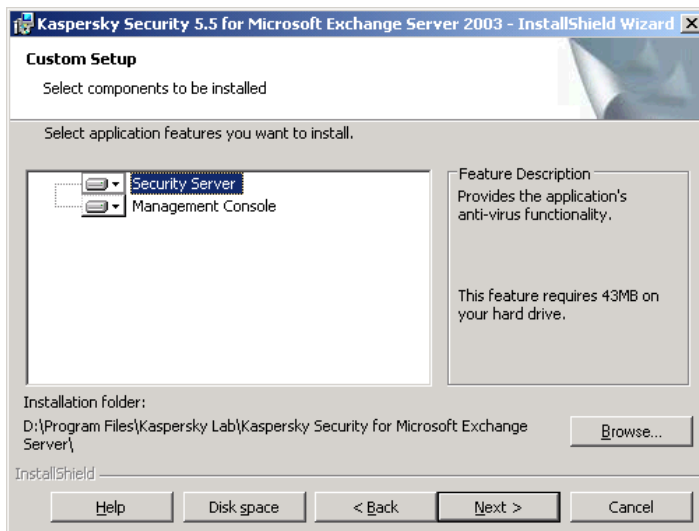


Figure 1. Selecting components for the installation

## Step 6. Enabling server protection

In the **Server protection** window, you will be offered to enable automatically the anti-virus protection and server protection against spam immediately after the wizard completes its work. You can do that manually using the application Management Console (see section 6.2, page 51).

If the application performance at the level and with the parameters applied by default (see section 4.6, page 33) meets the requirements of your server, we advise to accept the option of automatic anti-virus protection startup after completion of the setup wizard.

Please keep in mind that by default all mailbox storage areas created on the server will be selected as protected storage areas. If the maximum number of protected mail accounts 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 14.5, page 122).

If you wish to adjust the application settings first, disable automatic activation of anti-virus and anti-spam protection in the respective checkboxes.

## Step 7. Copying files

In order to proceed with the setup, press the **Install** button in the wizard window. This will start the process of copying the application files to your computer.

## Step 8. Installing the license key

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

If you installed the Security Server component, a window prompting you to add a license key will be displayed after the installation is complete.

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 mailboxes;
- the license name, number and expiration date.

Install the key to ensure full functionality of the application. In order to do this, press the **Add** button and select the key file in the standard Microsoft Windows File Select dialog box.

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.

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

## 3.1.2. Reinstalling the application

Reinstallation of Kaspersky Security 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 reinstall the application, run the executable file from its distribution package and select the **Repair** option in the wizard window. This will reinstall Kaspersky Security using the settings of 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.

## 3.2. Removing the application

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

During the uninstallation process, a prompt will be displayed asking you to confirm stopping the Microsoft Exchange Information Store and the Microsoft Internet Information services. Agree to stop these services to let the uninstallation process complete its work correctly. Once the uninstallation process is complete, the initial status of these services will be automatically restored.

## 3.3. Upgrading from a previous version

If the installer detects that your business is running Kaspersky Security 5.5 for Microsoft Exchange Server 2003 (release version, MP1), you can upgrade it to Kaspersky Security 5.5 for Microsoft Exchange Server 2003 MP2.



You are advised to process objects in the Backup before upgrading.

In order to upgrade, run the setup executable file from the distribution package of Kaspersky Security. During the installation of Kaspersky Security, the wizard will ask you to confirm removal of previously installed application. It will be uninstalled automatically.

During an upgrade of the application, the installer will automatically preserve the current settings for further use.

---

# 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 and the anti-spam protection features are enabled, they will start functioning immediately after the Microsoft Exchange Server is launched.

The operation of the application is controlled from the administrator's workstation – a computer where the Management Console is installed.



*In order to start the Management Console*

select the **Management Console** item in the programs group **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** from the standard **Start / Programs** Microsoft Windows menu. This programs group is created only on the administrator's workstations when the Management Console is installed.

## 4.2. Application interface

The user interface of the application is provided by the Management Console component. The Management Console is a dedicated isolated facility integrated into MMC.

### 4.2.1. Main application window

The main application window (see Figure 2) 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 used items of the main menu. The view pane displays the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** namespace in the form of the console tree, the results pane displays the list of all elements of the object chosen in the tree.

The **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** 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 2. Main application window

After a new server is added (see section 4.3, page 30), it is displayed in the console tree as a node **<Server Name>**. When the server is selected in the console tree (see Figure 2) the results pane will display hyperlinks, which can be used for application control and configuration.

- [General settings](#) – used for viewing general application's operation settings, license details and information about installed license keys, renewing the license and configuring the application operation diagnostics settings.
- [Anti-virus protection](#) – used for viewing and configuring the managed server's anti-virus protection settings
- [Anti-Spam protection](#) – used for viewing and configuring the settings of the server protection against unsolicited correspondence (SPAM).
- [Updates](#) – used to configure settings for the anti-virus and content filtration database update service, to set up an automatic update schedule and to update databases manually.

If the connection to the server has been established the node will include nested folders; each of these folders is intended for management of a specific application feature:

- **Notification templates** – for configuring notifications about infected or suspicious objects and messages containing spam detected during the 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 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 that opens after right-clicking an object with the mouse.

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
<b>Kaspersky Security 5.5 for Microsoft Exchange Server 2003</b>	<b>Add server</b>	Add a new Exchange server with the Security server installed to be managed via the console.
<b>&lt;Server name&gt;</b>	<b>Disconnect from the server</b>	Disconnect from the currently selected server.
	<b>Connect to the server</b>	Establish a connection with the currently selected server.
	<b>Remove the server from the console tree</b>	Remove the selected server from the view pane.

<b>Notification templates</b>	<b>New notification</b>	Create and configure a new notification template about infected and suspicious objects revealed by a scan and about messages containing spam.
<b>Backup storage</b>	<b>New filter</b>	Create and configure a new filter used to search for objects located in the backup storage.
	<b>Properties</b>	Configure general Backup parameters.
<b>Report templates</b>	<b>New report</b>	Create a new report template.
	<b>Properties</b>	Configure general parameters of report generation.
	<b>Clear report statistics</b>	Delete contents of the statistical database on program operation used for creating reports.
<b>Virus outbreak counters</b>	<b>New counter</b>	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 objects.

Using the **Create a report** command you can create a report based on the selected template.

The **Get file** command allows you to obtain the original copy of the object that had been saved before it was processed by the application. **Send file for analysis** – send an object from the Backup storage to Kaspersky Lab for analysis (the action is possible for infected or suspicious objects only).

**Send message to recipients** – send the message that was deleted or rejected by the spam scan to recipients.

## 4.3. Creating the list of managed servers

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



*In order to add a server to the list of managed servers:*

1. Select **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open the shortcut menu and select the **Add server** command or a similar item from the **Action** menu. This will open the **Add server** window (see Figure 3).

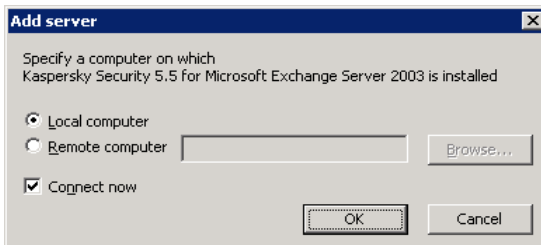


Figure 3. The **Add server** dialog box

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 computer name in the entry field. You can enter the name manually; to do this, specify one of the following:
  - IP address;
  - full domain name (FQDN in the following format **<Computer name>.<DNS-domain name>**);
  - computer's name in the Microsoft Windows network (NetBIOS name);

or select the computer from the list using the **Browse** button.



Later on, the Management Console will use this name to establish connection with the Security Server.  
The connection is established using DCOM protocol.

In order to establish connection between the Management Console and Kaspersky Security when adding the server, check the **Connect now** box (details see section 4.4, page 31).



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

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 node structure will include nested folders: **Notification templates**, **Backup storage**, **Report templates** and **Virus outbreak counters**. If the connection has not been established or could not be established you can connect to such server manually (see section 4.4, page 31).



*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 **Remove the server from the console tree** command or use a similar 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 Security 5.5 for Microsoft Exchange Server 2003 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 be able to connect to the Security Server, the user must have the local administrator rights for the computer to which the connection is attempted.

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



*In order to connect to the Security Server:*

select the node that corresponds to the necessary server in the console tree, open the shortcut menu and select the **Connect to the server** command or use a similar 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 structure will include folders **Notification templates**, **Backup storage**, **Report templates** and **Virus outbreak counters**.

If the connection could not be established, the application will display a warning with the indication of the problem and a suggestion to connect next time the Management Console is started.

One Security Server can have several Management Consoles connected to it. In this case, working with the same server from several consoles, you should regularly update information on each console. In order to do this, use the **Refresh** command available via the shortcut menu or the similar command in the **Action** menu.

## 4.5. Minimum required configuration

After the installation, the application will start working with the minimum set of parameters, 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 where 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 (see section 5.4, page 43).

In order to ensure full functionality of the mail server protection, it is necessary to configure settings used to notify the administrator or other users about the events occurred and about the virus outbreaks threat (see Chapter 11, page 93).

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

Exchange server protection against malware and SPAM starts operating immediately after the Security Server component is installed. The default operation mode of the application provides for the following:

- The application will scan objects for the presence of currently known malicious software (with the standard anti-virus protection level applied);
  - the body of the message and attached objects of any format will be scanned, except for container objects 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 Security 5.5 for Microsoft Exchange
Server 2003.
```

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 its copy (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:

```
A suspicious object (possibly %VIRUS_NAME%) has
been detected. File (%OBJECT_NAME%) was deleted
by Kaspersky Security 5.5 for Microsoft
Exchange Server 2003.
```

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 corrupted object is detected, the application will save its copy (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 Security 5.5 for Microsoft Exchange
Server 2003. File was password-protected or
corrupted.
```

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


- Messages received by Exchange server via SMTP protocol, will be scanned for SPAM:
  - the maximum time allowed for scanning 1 object is 200 seconds;
  - when formal messages (for example, messages automatically generated by mail bots) or messages that do not contain SPAM are detected, these messages will be delivered intact to the **Inbox** of the user's e-mail client.
  - when a suspicious message, which possibly contains SPAM, or message containing obscene words or message definitely containing SPAM are detected, such message will be moved to the **Junk E-mail** folder of the user's e-mail client.
- All public folders, all storage areas created on the Exchange Server and all users registered with this mail server will be protected.
- Mail traffic routed by the Exchange server will not be scanned.
- The anti-virus and content filtration databases are updated hourly via internet from the Kaspersky Lab's HTTP and FTP servers.
- The administrator will not be notified about objects detected during the scan.
- 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 protection system are created on the first day of each month and cover last 30 days.

## 4.7. Verifying the application performance

After Kaspersky Security is installed and configured, we recommend verifying the correctness of its settings and operation:

- using a test "virus" and its modifications (see section 4.7.1, page 35);
- using a test SPAM message (see section 4.7.2, page 36).

### 4.7.1. Testing the anti-virus protection system

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](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 Security 5.5 for Microsoft Exchange Server 2003 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 the application 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 the anti-virus component 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-	An error corresponding to detection of a corrupted object.
CURE-	Infected (can be cured). The object will be disinfected; the text of the "virus" body will be replaced with the word "DISINFECTED".
DELE-	Infected (cannot be cured). 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[4\PZX54(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 *eicar\_dele.com* (assign names to all the modified "viruses" in the same manner).

The second column of this table contains the types of objects identified by the anti-virus application after you have added a prefix. The actions for each type of objects are defined by the anti-virus scan settings (see section 6.5, page 57) customized by the administrator.

## 4.7.2. Testing the anti-spam protection system

You can use a test message identified as SPAM to test the anti-spam server protection.

The subject of the test message must contain the following line: `Spam is bad do not send it.`

When such message arrives at Exchange Server, Kaspersky Security will assign it SPAM status and will process it applying the action specified for this type of objects by the administrator (see section 7.2, page 67).

---

# CHAPTER 5. UPDATING THE ANTI-VIRUS AND THE CONTENT FILTRATION DATABASES

Users of Kaspersky Lab's products can update:

- *anti-virus database* used to detect malicious programs and disinfect infected objects. Anti-virus database files contain description of all currently known malicious programs and disinfection methods for objects infected with such malware as well as the description of all potentially dangerous software (riskware);
- *content filtration database*, used for the linguistic analysis to detect SPAM in the message body and attachments. The content filtration database contains examples of spam messages as well as words and phrases characteristic of SPAM messages.



It is extremely important to keep your databases up-to-date. We recommend that you update your databases immediately after your application is installed because the databases included into the distribution kit will be out-of-date by the moment you install your application.

These databases are updated on an hourly basis on the Kaspersky Lab's server. We recommend that you setup automatic updates with the same frequency (see section 5.2, page 40).

The anti-virus and the content filtration databases can be updated from the following sources:

- from Kaspersky Lab's internet update servers;
- from a local updates' source - a local or a network folder.

The updating is performed manually or according to the schedule. After the files are copied from the specified source of updates, the application automatically connects the databases received and performs mail scan for viruses and spam using these new databases.



*In order to review the status of the databases and modify the updating settings,*

In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Servers 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Up-dates](#) link in the results pane.

You can do the following in the anti-virus and content filtration database updating settings window:

- review the database status and launch the update manually (see section 5.1, page 39);
- schedule automatic updates (see section 5.2, page 40);
- specify the updates source (see section 5.3, page 41);
- configure the network connection settings (see section 5.2, page 40).



You can setup different updates parameters for the anti-virus database and for the content filtration database.

## 5.1. Manual updating



*In order to update the anti-virus and the content filtration databases in the manual mode,*

In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Servers 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Up-dates](#) link in the results pane.

The **General** tab in the **Updates** window (see Figure 4) that will open contains information about the currently used database version and the result of the last update.

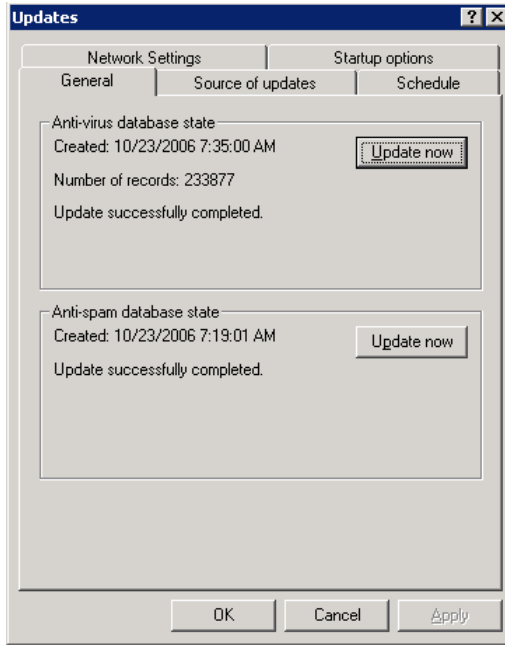


Figure 4. Configuring update settings.  
The **General** tab

In order to update the anti-virus database and content filtration database immediately, press the **Update now** button in the corresponding section. The application will launch the updating process using the selected settings.

## 5.2. Automatic updates



*In order to update the database in the automatic mode,*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Updates](#) link in the results pane.
2. Switch to the **Schedule** tab in the **Updates** window that will open.

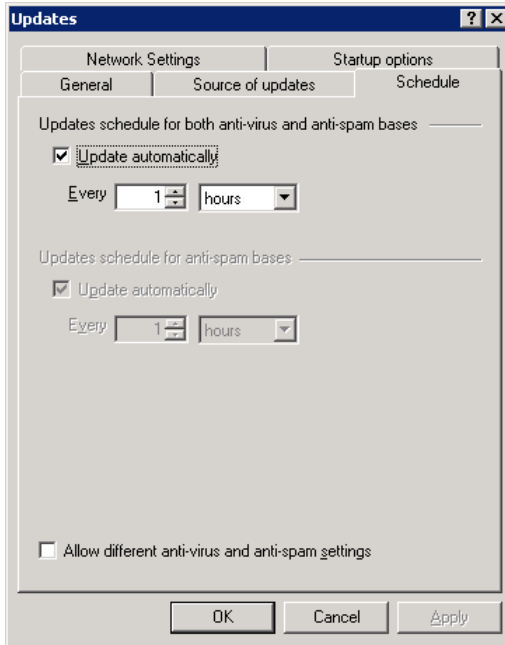


Figure 5. Configuring update settings.  
**Schedule** tab

In order to enable the automatic updates of the anti-virus and the content filtration databases, check the **Update automatically** box and set up the schedule for receiving updates. If the box is not checked, the databases must be updated manually (see section 5.1, page 39).

You can select different modes for updating the anti-virus and the content filtration databases. In order to do this, check the **Allow different anti-virus and anti-spam settings** box. This will divide the schedule setup window into two corresponding sections.

For example, you can create separate schedules for updating the anti-virus and the content filtration databases and disable the automatic updating feature for one of the two types.

## 5.3. Selecting the updates source

By default, the anti-virus and the content filtration databases are updated from the Kaspersky Lab's internet update servers.

Additionally, you can configure the updates to be downloaded from a HTTP, FTP server or a network folder.

If you have Kaspersky Administration Kit (the centralized Kaspersky Lab's applications management system) installed in your corporate network, then the databases updates received by the Administration Servers will be copied to a public folder (details see Kaspersky Administration Kit Guide). This folder can be used as the updates source for your copy of Kaspersky Security 5.5 for Microsoft Exchange Server 2003.



*In order to select a different anti-virus and content filtration databases updates source:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Updates](#) link in the results pane.
2. Switch to the **Source of updates** tab in the **Updates** window that will open (see Figure 6) and specify the updates source required:
  - **Updates' servers of Kaspersky Lab** - Kaspersky Lab's HTTP- and FTP internet servers where new updates are uploaded every hour (default option).  
Below you can specify the update server of Kaspersky Lab, which is nearest to your geographical location. In order to do that, select your current location from the respective drop-down list. That will help decrease the time necessary to download updates and increase their transfer speed.
  - **HTTP-, FTP-server or network folder** - a network or a local folder or the Kaspersky Administration Kit Administration Server where the updates downloaded from the internet are copied. If you selected this option, enter the path to the folder in the entry field or select the folder in the standard Microsoft Windows dialog box that opens by pressing the **Browse** button.

You can specify different updates sources for the anti-virus database and the content filtration database. In order to do this, check the **Allow different anti-virus and anti-spam settings** box. This will divide the source selection window into two corresponding sections.

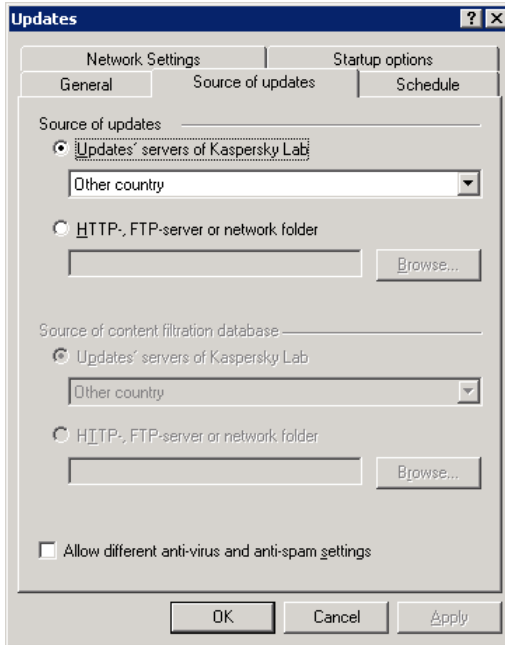


Figure 6. Configuring update settings.  
The **Source of updates** tab

## 5.4. Configuring the connection settings



*In order to view/modify the network connection settings:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Updates](#) link in the results pane.
2. Switch to the **Network Settings** tab (see Figure 7) in the **Updates** window that will open and configure 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: address and number of the port used for connection.

- If you use a password in order to access the proxy server, specify the proxy user's authentication settings. In order to do this check the **Proxy server authentication** box and fill in the **Name** and the **Password** fields.
- 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.
- Check the **Use passive FTP mode** box if your server has a firewall and you cannot connect to the required FTP server in the active mode.

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

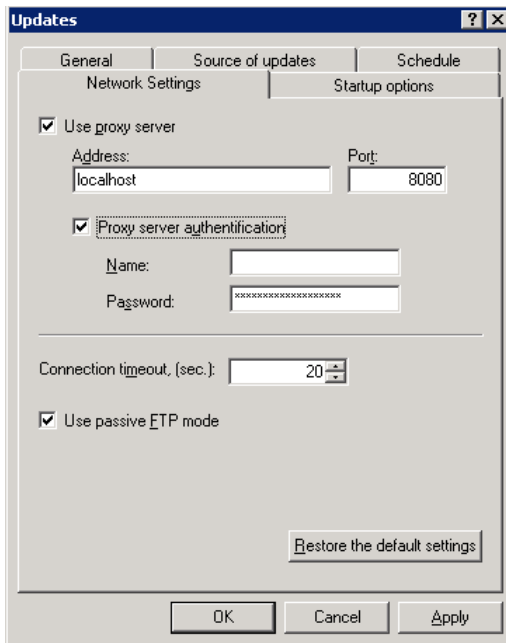


Figure 7. Configuring update settings. The **Network Settings** tab

## 5.5. Running updates under a different user account

Kaspersky Security program updates can be run under a different user account. This feature is disabled by default, and tasks are run under the system profile.

For example, you might want to run a task under a different user account if you are updating from a source that the computer does not have access to (such as a network update folder) or from a source where it does not have authorized user privileges to the proxy server. You can use this feature to run updates with another profile that has those rights.



*To configure an update to start under a different user profile:*

1. In the main program window, select **Kaspersky Security 5.5 for Microsoft Exchange Server 2003**, from the console tree, open it, select the node that corresponds to the server needed, and click the [Updates](#) hyperlink in the results pane.
2. In the **Updates** window that opens, go to the **Startup options** (see Figure 8) and enter the data for the account under which you want to start the update (username, password, confirm password). You can enter the username manually or add an account in the standard Microsoft Windows window that opens when you click **Browse**.

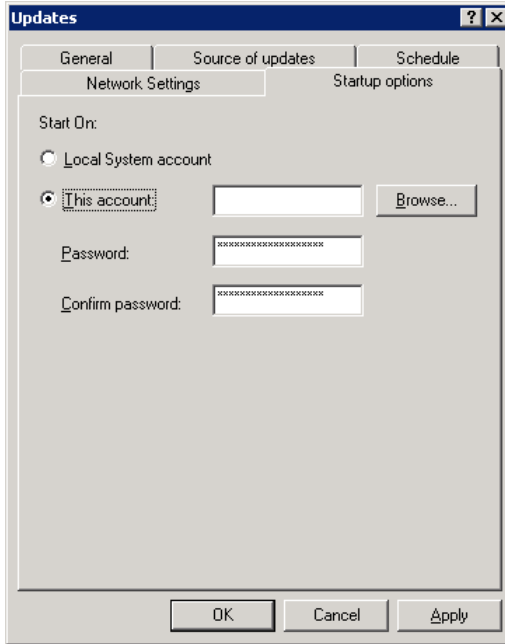


Figure 8. Configuring update settings.  
The **Startup options** tab

---

# CHAPTER 6. ANTI-VIRUS PROTECTION

The main task of Kaspersky Security for Microsoft Exchange Server 2003 is to perform an anti-virus scan of mail traffic and to disinfect 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 6.1, page 49), the application allows detection of:

- malicious objects;
- potentially dangerous 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 and all traffic routed by the Exchange server via SMTP protocol. In order to decrease the load on the server, you can disable the scan of the routed mail traffic (details see section 6.3, page 53).

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 e-mail messages based on the settings configured:

- 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 section 6.4, page 56);
- 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 section 6.1, page 49), then starting and stopping of the traffic scan will be performed simultaneously with the starting and stopping of the Microsoft Exchange Server.

Kaspersky Security does not scan messages created by protected users in the **Public folders** of unprotected Exchange servers. If messages are transferred from **Public folders** of an unprotected area to a protected one, the application will scan them. In case of data replication in protected and unprotected areas changes will not be synchronized.

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 (if the background storage scan is enabled). 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 section 6.6, page 62).



If the background scan mode is enabled for the application used on a servers cluster, the background scan can start 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 configured, 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 in 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 Security differentiates between simple objects (an executable file, a message with a simple attachment) and containers (consisting of several objects, for example, an archive or a message with any message attached to it).



When scanning multiple-volume archives, Kaspersky Security treats and processes each volume as a separate object. In this case, the application can detect malicious code only if such code is fully located in one of the volumes. If a virus is also divided into parts, then it cannot be detected when only part of the data is loaded. In this situation, the malicious code may propagate after the object is restored as one entity.

Multiple-volume archives can be scanned after they are saved to the hard drive by the anti-virus application installed on the user's 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 mask or files specified by type (details see section 6.3, page 53).

Kaspersky Security 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 9 objects up to 1 MB each in the computer's RAM without using the disk subsystem (details see section 8.1, page 72).



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 anti-virus applications installed in the enterprise local network.

## 6.1. Anti-virus protection levels

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 allows detecting and preventing the penetration of the following types of objects through the mail server:

- All currently known malicious programs.
- 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 (including porn websites);
  - automatic porn files downloading programs;
  - keyboard spies;
  - password hacking programs;
  - backdoor programs.
- Joke programs and programs with "bizarre" content or form that affect the system in a way that cannot be qualified as beneficial. This type of software includes:

- programs that cause unexpected video or sound effects;
- programs that cause problems in the system operation;
- virus simulators.
- 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 application as a behavior characteristic of malicious or potentially dangerous software. Examples of such software are backdoor and remote surveillance software.

Categories of objects detected by Kaspersky Security 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 **b** in the list above.
- **Redundant anti-virus protection:** protection against all currently known malicious programs and potentially dangerous software included under **b**, **c**, and **d** in the list above.

## 6.2. 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 or stopped 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 section 6.6, page 62).

Scan of objects is performed according to the determined anti-virus protection level.

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 9) window that will open.

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

- **Disabled** - in order to disable mail anti-virus protection
- **Standard anti-virus protection, Extended anti-virus protection or Redundant anti-virus protection** - in order to enable mail anti-virus protection using the corresponding level (see section 6.1, page 49).



The use of extended or redundant anti-virus protection level may affect the speed of the program's operation. Besides, some programs may be referred to potentially dangerous programs when transferred by mail, and so they may be deleted or blocked, depending upon the application settings (see section 6.5, page 57).

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

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.

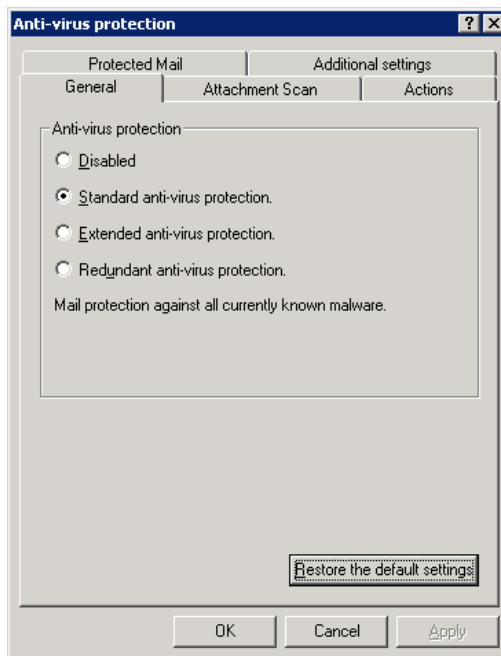


Figure 9. Enabling the anti-virus protection



We do not recommend disabling the server's anti-virus protection by disabling the Kaspersky Security 5.5 for Microsoft Exchange Server 2003 service manually using the **Computer Management / Services** snap-in.



*If you need to disable Kaspersky Security 5.5 for Microsoft Exchange Server 2003 service manually, do the following:*

1. Disable the anti-virus mail protection using the **Management Console** (see above).
2. Disable the anti-spam server protection using the **Management Console** (see section 7.1, page 66).
3. Restart the Microsoft Exchange Information Store and IIS Admin services.
4. Specify the **Disabled** startup type for the service of Kaspersky Security 5.5 for Microsoft Exchange Server 2003.



*In order to start the application after the automatic startup of the Kaspersky Security 5.5 for Microsoft Exchange Server 2003 service has been disabled, do the following:*

1. Specify the **Auto** startup type for the service of Kaspersky Security 5.5 for Microsoft Exchange Server 2003.
2. Enable the anti-virus mail protection using the Management Console (see above).
3. Enable the anti-spam server protection using the Management Console (see section 7.1, page 66).

## 6.3. 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 scanning the attachments.*



*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 10) window that will open.

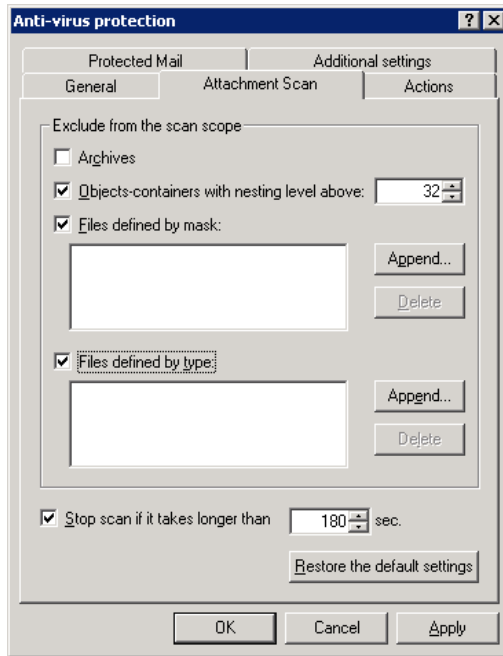


Figure 10. Configuring restrictions for the attachment scan

3. In the **Exclude from the scan scope** group, specify objects that you wish to exclude from the anti-virus scan scope:
  - **Archives** – exclude archives from the scan scope.
  - **Objects-containers with nesting level above...** – exclude from the scan scope containers with the nesting level exceeding the value specified in the field to the right.



Since archives are one of the types of containers, the restrictions applied to the scan of archives and containers are inter-related.

If you impose a restriction to the scan of containers, archives will then be scanned only to the specified nesting level (if they are not explicitly excluded from the scan scope).

However, excluding archives from the scan scope will not affect the scan of containers.

There are objects that cannot be infected. In order to reduce the load on the server while the anti-virus scan of mail messages is in progress, we recommend specifying types and/or names of such attachments and ex-

cluding them from the scan scope. In order to do this, specify exclusions by the file type or using a mask:

- **Files defined by mask.** Using the **Append** and **Delete** buttons, create the list of exclusion masks. When adding an exclusion in the **Adding a mask** window (see Figure 11), enter the exclusion mask into the corresponding field.

Examples of allowable masks:

- **\*.txt** – all files with mask *\*.txt*
- **\*.tx?** – all files with mask *\*.tx?*
- **test** – all files with name *test*

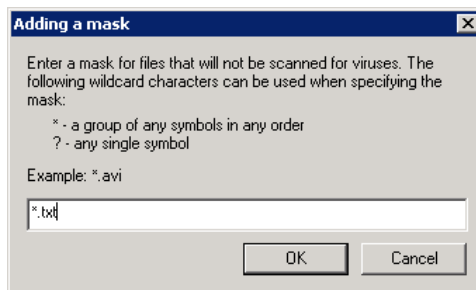


Figure 11. Specifying the masks for files to be excluded from the scan scope

- **Files defined by type.** Using the **Append** and **Remove** buttons, create the list of attachment types that will be excluded from the scan scope. When adding an exception in the **Adding a type** window (see Figure 12), select a type from the drop-down list.

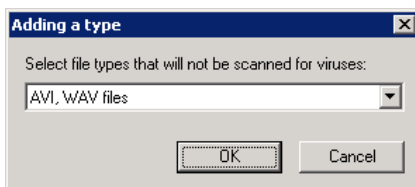


Figure 12. Specifying the type of files to be excluded from the scan scope

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.

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

## 6.4. Scanning of routed e-mail traffic

In order to reduce the load on the server in the traffic protection mode, we recommend that mail traffic routed by the server, shall not be scanned.



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

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** 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 **Protected Mail** (see Figure 13) tab in the **Anti-virus protection** window that will open.
3. Check the **Do not scan routed mail** box in the **Routed mail** group of boxes (checked by default).

While enabling scanning of routed mail, please make sure that the anti-virus protection for the Microsoft Exchange Server storage, containing the System Attendant mailbox, is enabled. Otherwise traffic will not be scanned and all routed mail will be blocked in the queue of Messages pending submission.

In addition, you are advised to restart Microsoft Internet Information Services using the **iisreset** command after you enable scanning of routed mail.

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

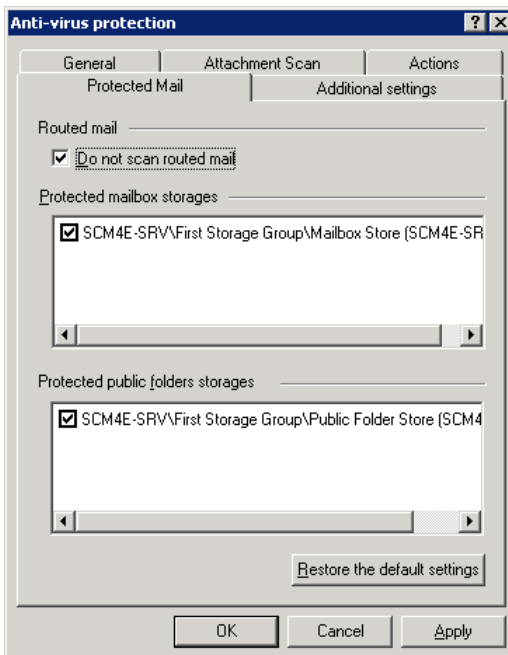


Figure 13. Excluding transit traffic from the scan scope

## 6.5. Selecting actions to be performed with 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.

Depending on the object's status different actions will be applied.

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 was 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* – replace the infected message body with text created using the corresponding replacement template and change the name and extension of the infected attached objects. Such renamed objects will have *.txt* extension.



The name change affects attached objects only; if a virus was detected in the message body, no renaming is performed.

- *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.



If the infected attachments are disinfected, replaced with text or re-named, 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 regularly.

Before the processing, a copy of the object can be saved in the backup storage so that later it can be restored or sent to Kaspersky Lab for analysis (see Chapter 8, page 72).

The application can send notification about the object detected to the administrator or to other users or register such event in the Microsoft Windows event log (see Chapter 10, page 86 and Chapter 13, page 111).

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. The **Replace message body with text and rename attachments** action will be assigned to objects with a different status, and the text of the informative

message will include the name of the virus detected and the name of the infected object.



If an object attached to the message was processed (disinfected, deleted, replaced) by Kaspersky Security, 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 rules for processing 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 14) that will open.

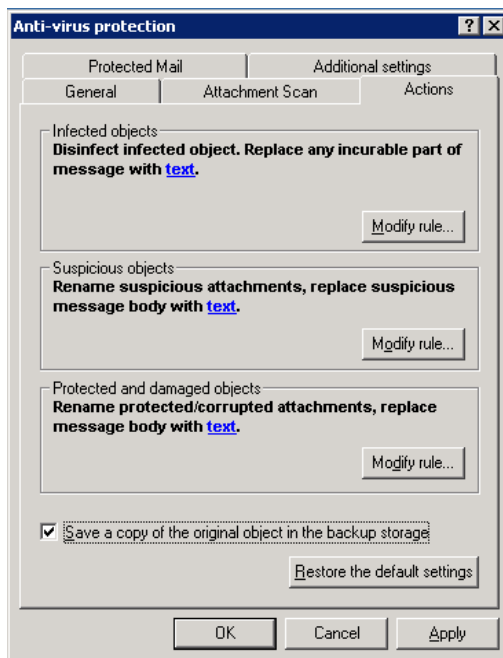


Figure 14. Configuring actions to be applied to infected objects

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

- Determine the rule for object processing 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.
- In the window that will open (see Figure 15) select actions from the list.

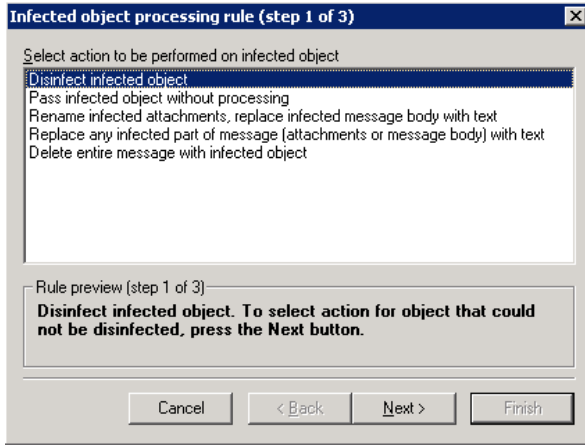


Figure 15. Creating the replacement template

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.

- If you selected disinfection as the action to be performed with the object, during the next step you will be offered to determine the procedure to be used to process objects that could not be disinfected (see Figure 16).

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

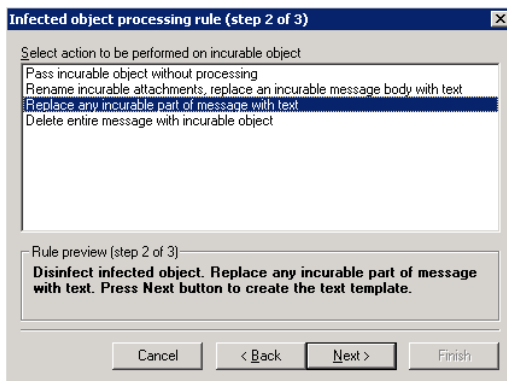


Figure 16. Selecting an action to be performed with an object that could not be disinfectd

6. If you selected one of the actions that involve replacement of the object with text, you will be offered to create a replacement template (see Figure 17). 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 description of the macros in the list is provided in Appendix A, page 160.

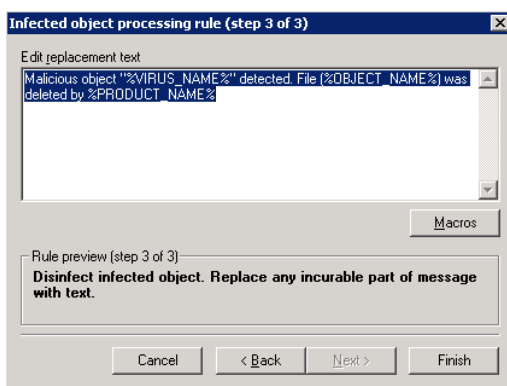


Figure 17. Creating a replacement template

In order to close the 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 (see Figure 14).

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

## 6.6. Background scan

Kaspersky Security 5.5 for Microsoft Exchange 2003 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 (see section 14.5, page 122).



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

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** 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 18) that will open.

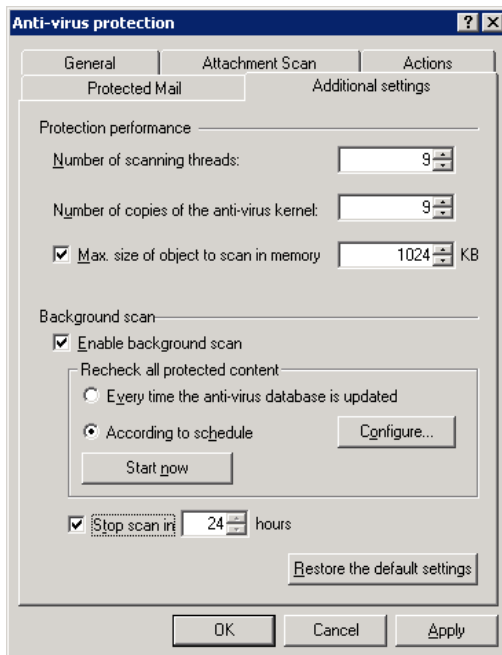


Figure 18. Configuring background scan settings and anti-virus protection performance

3. Check the **Enable background scan** box (unchecked by default) and specify the desired scan launch option:
  - **Every time the anti-virus database is updated** – launch the scan every time the anti-virus database is updated.
  - **According to schedule** – launch the scan according to the specified schedule. Specify the mode and the time for the scan in the window that opens by pressing the **Configure** button (see Figure 19).

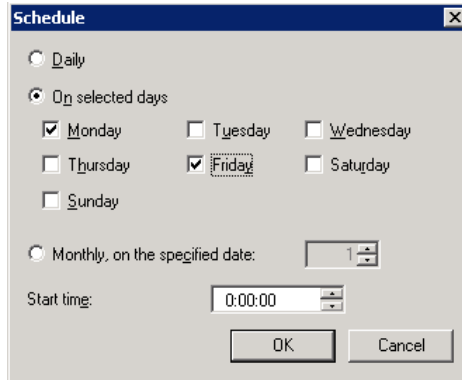


Figure 19. Creating the background scan schedule

If you need to start the scan immediately, press the **Start now** button (Figure 18).

4. 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.

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

---

# CHAPTER 7. ANTI-SPAM PROTECTION

One of the main tasks of Kaspersky Security 5.5 for Microsoft Exchange Server 2003 is protection of mailboxes and public folders of the Exchange server against unsolicited e-mail messages (SPAM).

The anti-spam scan module filters the incoming e-mail messages while they are being received via SMTP protocols that is, before the messages get into the users' mailboxes.

## The application scans for spam:

- Internal and external traffic generated by SMTP clients using anonymous authentication on the server.
- Messages arriving at the server via anonymous external connections (front-end server).

## The application does not filter spam in:

- Internal LAN traffic.
- External traffic arriving at a server via authenticated sessions.

Each e-mail message will be scanned for the presence of spam attributes. In order to do this, the application checks, **first of all**, various message attributes: the sender's and the recipient's addresses, message size, headers (including the *From* and the *To* headers).

**Secondly**, anti-spam *content filtration* is used to analyze the content of the message (including the *Subject* header) and the attached files<sup>1</sup>. The application uses unique linguistic and heuristic algorithms based on the comparison of actual messages with the sample messages and on the deeper analysis of the text, formatting features and other attributes of the e-mail messages.



The content filtration database is continuously updated in the linguistic laboratory based on the everyday monitoring of spam sources. Therefore, in order to maintain the application in the up-to-date state, the database shall be updated on an hourly basis (see Chapter 5, page 38).

Messages, in which no SPAM has been found by the anti-spam filtering, will be delivered intact to the user's mailbox. Other messages that were related to unsolicited correspondence are assigned one of the four categories of SPAM:

---

<sup>1</sup> Attachments of the following formats are scanned: Plain text, HTML, Microsoft Word, RTF.

SPAM, suspicious message, formal message, obscene message (details see section 1.1, page 7).

Messages in which traces of SPAM have been detected, will be processed by applying actions described in section 7.2, page 67.

## 7.1. Enabling/disabling anti-spam protection



*In order to enable/disable anti-spam protection:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-Spam protection](#) link in the results pane.
2. Check/uncheck the **Enable anti-spam** box in the **General** tab (see Figure 20) in the window that will open.

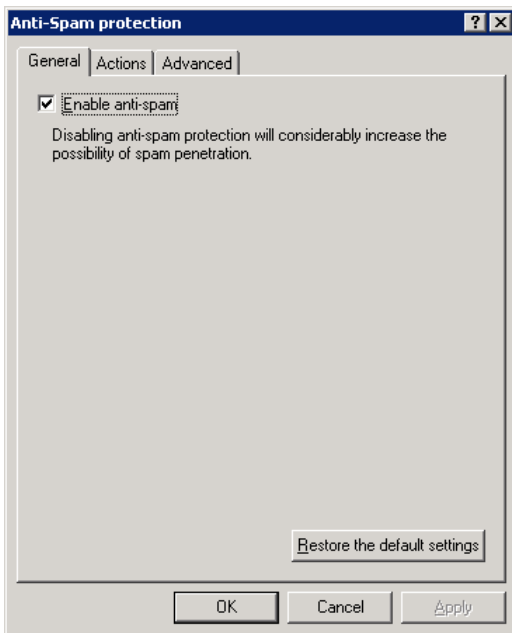


Figure 20. Configuring anti-spam protection settings.  
The **General** tab

When you click the **Restore the default settings** button, Anti-Spam will be enabled.



We do not recommend disabling Anti-Spam by disabling the Kaspersky Security 5.5 for Microsoft Exchange Server 2003 start function manually through **Manage computer / Services** (see section 6.2, page 51).

## 7.2. Selecting the action to be performed with the message



*In order to select an action to be performed with a message in which spam has been found,*

In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-Spam protection](#) link in the results pane.

Specify the rules for processing messages for each type of SPAM in the **Actions** tab (see Figure 22) of the window that will open:

- *Skip* – deliver the message into the user's **Inbox**. By default this action is applied to messages that do not contain spam attributes and to formal e-mails.
- *Move to the Junk E-mail folder* – deliver message to a special folder of the e-mail client on the recipient's computer. The action is used by default for all categories of spam messages except for formal ones.

This action is only available in Microsoft Office Outlook 2003. In other mail clients, e-mails will be moved to the *Inbox* folder. To identify e-mails containing signs of spam, we recommend flagging subjects with special markers in the *Inbox* folder (see below).



Note that e-mail processing rules assigned in the mail client are carried out after the action *Move to the Junk E-mail folder*. For example, if the rule requires automatic deletion of all messages from the **Junk E-mail** folder, then the message will be deleted. No copies of this message will be saved to the backup storage.

- *Decline* - block the message delivery to the recipient.



The declined message, sent via SMTP protocol by the user within the corporate network, will remain with an error code in the **Sent Items** folder. Such message can only be deleted manually.

- *Remove* - delete the message.

In addition to the action **Skip** or **Move to the Junk E-mail folder** you can flag subject lines with special markers. For example, for e-mail in the category "e-mails containing spam", the marker **[!!! SPAM]** can be added to the subject line.

To add a marker, click **Mark**. In the window that opens (see Figure 21) check the **Add label to the message subject** checkbox, enter the text of the marker in the field below, and specify the position of the marker in the subject line of the e-mail.



Please note that only Latin characters can be used in the text of the marker.

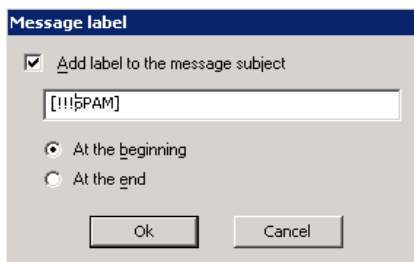


Figure 21. Adding markers to the subject line of the message

By default, if a message is declined or deleted, a copy of such message is saved to the backup storage (see Chapter 6, page 47). If necessary, you can restore the message from the backup storage or forward it to recipients unchanged. If you do not want copies to be saved, uncheck the **Save a copy of the original object in the backup storage** box.

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

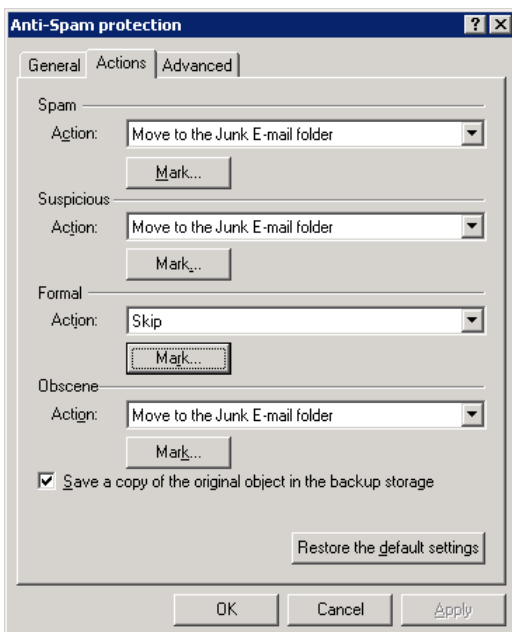


Figure 22. Configuring Anti-Spam settings.  
The **Actions** tab

## 7.3. Configuring TCP/IP settings

Anti-spam mail scan is performed by the service using the TCP/IP settings. These settings will be applied automatically during the program's installation.

In case of a conflict with other applications installed on your computer using the same port for TCP/IP, we recommend changing it. In order to do this, enter the appropriate values in the **TCP/IP settings** section in the **Advanced** tab of the **Anti-Spam protection** window (see Figure 23).

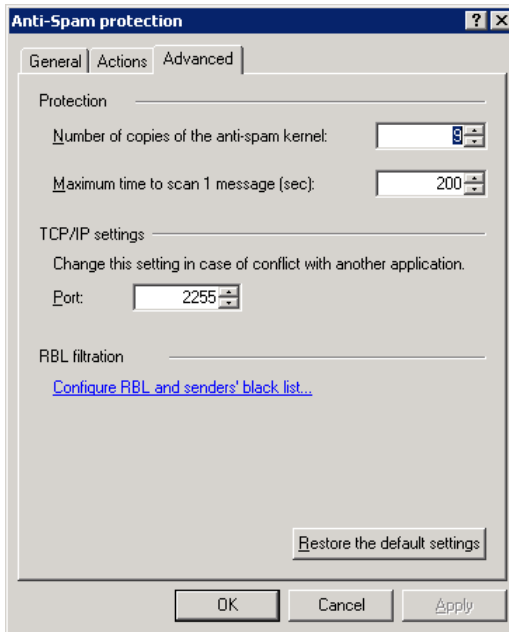


Figure 23. Configuring anti-spam protection settings.  
The **Advanced** tab

## 7.4. Configuring e-mail filtration

Kaspersky Security does not have its own e-mail filtration using Realtime Block List (RBL) or e-mail addresses. This function is carried out by Microsoft Exchange Server 2003 features.

Microsoft Exchange Server 2003 supports filtration of connections and recipients. These features can be used to reduce the amount of spam sent to organizations.

Connection filtration allows the Exchange Server to access block lists and determine if the computer sending an e-mail is on those lists. Exchange Server can also be used to specify exclusions from block lists.

In addition, Exchange Server can be used to create recipient filters that restrict delivery of e-mail to defined recipients in the organization or beyond.



*To configure connection filtration:*

1. Open **Exchange System Manager**.
2. Open the **Global Settings** node, select **Message Delivery**, and select **Properties** from the context menu.
3. In the window that opens, select the **Connection filtering** tab.

You can read more about creating, configuring, and applying connection filters in the documentation or help files of Microsoft Exchange Server 2003.



*To configure recipient filtration:*

1. Open **Exchange System Manager**.
2. Open the **Global Settings** node, select **Message Delivery**, and select **Properties** from the context menu.
3. In the window that opens, select the **Recipient Filtering** tab.

You can read more about creating, configuring, and applying recipient filters in the documentation or help files of Microsoft Exchange Server 2003.

---

# CHAPTER 8. APPLICATION'S OPERATION EFFICIENCY

Kaspersky Security for Microsoft Exchange Server 2003 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.

Additionally, you can fine-tune various efficiency levels of anti-virus and anti-spam protection.

## 8.1. Anti-virus protection efficiency



*In order to configure the anti-virus protection efficiency settings:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** 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 18) that will open.
3. In the **Protection performance** group of fields specify the desired parameters, which determine the performance of anti-virus protection:
  - The number of streams that contain objects to be scanned. Microsoft recommends that the value of this setting equals  $2 \times \text{number of processors} + 1$ . This is the default value for this parameter.
  - The number of instances of the anti-virus kernel running simultaneously (the default value is  $2 \times \text{number of processors} + 1$ ).
  - 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 **Max. size of object to scan in memory** box and specify the maximum size in

kilobytes. By default, the box is checked and the size of the object is 1024 KB.

## 8.2. Anti-spam protection efficiency



*In order to configure the anti-spam protection efficiency settings:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [Anti-Spam protection](#) link in the results pane.
2. Go to the **Advanced** tab in the **Anti-Spam protection** window (see Figure 23) that will open and specify the values for the efficiency settings:
  - Specify the number of kernel instances that are running simultaneously in the **Number of copies of the anti-spam kernel** field (the default value is *2 x the number of processes + 1*).
  - Specify the time restriction for processing each message in the **Maximum time to scan 1 message (sec)** field. The default value is 200 seconds.

---

# CHAPTER 9. BACKUP COPYING

Kaspersky Security for Microsoft Exchange Server 2003 allows saving a backup copy of an initial object before processing. For example, before an attempt to disinfect or delete such object or before declining or deleting a message containing SPAM attributes, an initial copy can be saved to the *backup storage*.

Later on objects located in the backup storage may be:

- **restored** - in order to obtain information contained in the object. Additionally, you can restore the infected object and try to scan it with the file anti-virus using an updated anti-virus database (see section 9.3, page 80).
- **deleted** - (see section 9.6, page 82).
- **sent to be inspected by Kaspersky Lab** (only for suspicious files containing a modification of a known virus or code of a virus still unknown). Our specialists will analyze the file, attempt to recover the data, and if it turns out that the file is infected with malicious code, make an entry in the anti-virus database. Then, when you scan this file with File Anti-Virus using the updated database, you can disinfect it and maintain the integrity of the data in it (see section 9.4, page 81).
- **sent to recipients** unchanged (only for e-mails deleted or rejected by a spam scan). For more, see section 9.4, page 81.



A backup copy of the object will be created only if the **Save a copy of the original object in the backup storage** box in the anti-virus protection settings (see section 6.5, page 57) and anti-spam settings (see section 7.2, page 67) is checked.

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).

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 500 MB. 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 no enough free disk 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 section 9.1, page 75), configuring backup storage parameters (details see section 9.7, page 83) and managing backup copies (details see section 9.3, page 80, section 9.4, page 81 and section 9.6, page 82) features are available via the **Backup Storage** service folder (see Figure 24). 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 section 9.2, page 77). Filters, created for the backup storage, can be viewed in the **Backup Storage** folder as subfolders under the names assigned by the administrator when the filters were created.

## 9.1. Viewing the backup storage



*In order to view the backup storage:*

In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and select the **Backup storage** folder in the console tree.

A table containing the full list of all objects contained in the backup storage will appear in the results pane (see Figure 24).

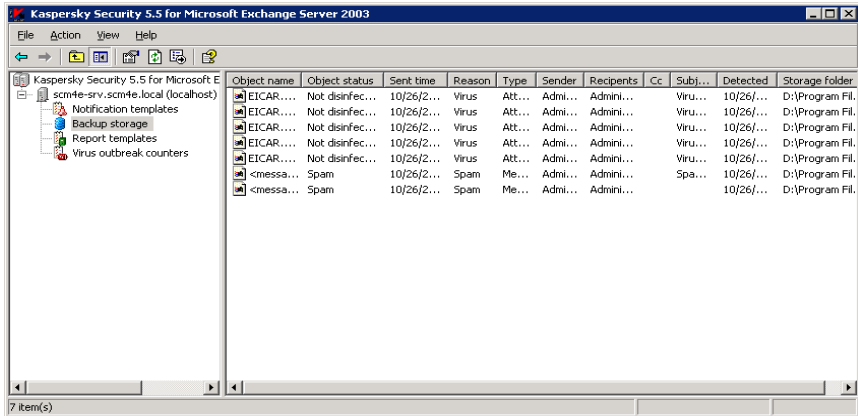


Figure 24. Viewing the backup storage

In addition to the standard e-mail message attributes (**Sender, Recipients, Cc, Subject, Sent time**), this table will contain the following information for each object:

- **Object name.** Attachments will retain their original names, while the message body will be saved as **<message body>** (result of anti-virus scan) or **<message>** (result of spam scan).
- **Object status.** The status assigned to the object as a result of an anti-virus scan (see section 6.5, page 57) or anti-spam scan (details see Chapter 7, page 65).



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

- **Detected.** Exact date and time when the object was detected by Kaspersky Security.
- **Reason.** The reason that has caused object addition to the backup storage.
- **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.

## 9.2. Backup storage filter

The use of filters allows performing 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. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and select the **Backup Storage** folder in the console tree.
2. Use the **New Filter** command in the context menu or the analogous item under the **Action** menu.
3. In the filter settings window that opens, assign e-mail filtration settings on the **Filter** tab (see Figure 25):
  - name, under which the filter will be included in the **Backup Storage** folder;
  - object status (several values can be selected).

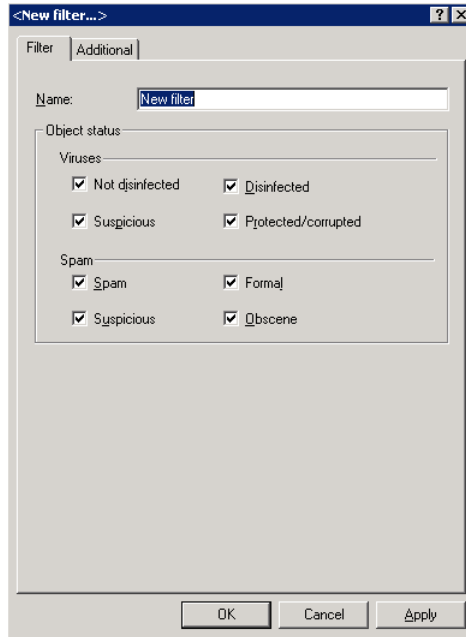


Figure 25. Creating a new filter.  
The **Filter** tab

4. On the **Additional** tab (see Figure 26) specify the values for the filter settings that will be used to search for objects in the backup storage. To configure settings, use the following file attributes:
  - o file type. E-mails may be filtered by type: **Message** (result of spam scan), **Message Body**, **Attachment** (result of anti-virus scan), or all types together;
  - o object name (only available if you select attachment filtering in the **Type** field);
  - o sender of the e-mail;
  - o recipient of the e-mail;
  - o recipient of e-mail copy;
  - o e-mail subject;
  - o time interval during which the e-mail was sent.

When completing the fields of the filter, you can use the wildcards – \* (any combination of characters) or ? (any character).

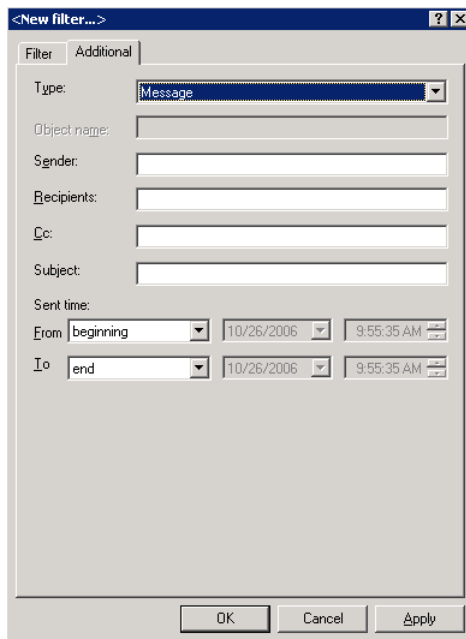


Figure 26. Creating a new filter.  
The **Additional** tab

5. After you are done with the filter settings, press the **Apply** or the **OK** buttons 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 complies with the filter criterion will be displayed in the results pane.

Later on you can alter the values of filter parameters or delete the filter using the shortcut menu commands or the **Action** menu items.



*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 25).

2. Modify the filter parameter values as required.
3. In order to apply the changes, press the **Apply** or the **OK** buttons. To exit without saving the changes, 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.



*In order to delete a filter:*

Select the name of the filter in the **Backup Storage** folder and use the **Delete** command from 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 parameters will still be available in the **Backup Storage** folder.

## 9.3. 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 24). You can use filter to search for the object (see section 9.2, page 77).
3. Open the shortcut menu and use the **Get file** command or the analogous item under the **Action** menu.
4. In a window that will open specify the folder to which you wish to save the object restored, and if required, enter or modify the object's name.
5. Before restoration a warning message will be displayed, asking 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 was first processed by the application. After the object is successfully restored, a corresponding notification is displayed on the screen.



We recommend restoring only those messages that contain spam attributes or that have **suspicious, protected or corrupted** status. A new scan of such objects using the updated databases 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!

## 9.4. Sending e-mails to recipients

E-mails can only be sent to the original recipients specified in the **To** field for objects deleted or rejected by a spam scan. Note that the e-mail will not be sent to the recipients listed in the **Cc** field.



*To send an e-mail to its recipients:*

1. In the main program window, select **Kaspersky Security 5.5 for Microsoft Exchange Server 2003**, from the console tree, open it, select the node that corresponds to the server needed, and select the **Backup storage** folder from the console tree.
2. Select the object to send from the table that displays the contents of the backup storage (see Figure 24). Use a filter to search for the objects (see section 9.2, page 77).
3. Open the context menu and select the **Send message to recipients** command or select the same item from the **Action** menu.



Warning: if more than one virtual SMTP server is installed on the computer, the e-mail will always be sent through the first server. Therefore, to send an e-mail correctly, the server must be configured to route e-mails to the necessary address.

## 9.5. Sending objects for analysis

The user can send for analysis to Kaspersky Lab only those objects that are suspected of being infected with a modification of a known virus or contain code of a virus that is known yet known.



*In order to send a suspicious object to Kaspersky Lab's experts for analysis,*

1. Select the **Backup Storage** folder in the console tree.
2. Select the object with the **suspicious** status you wish to send for analysis in the table displaying the content of the backup storage (see Figure 24). You can use filter when searching for the object (see section 9.2, page 77).
3. Open the shortcut menu and use the **Send file for analysis** command 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 notification confirming that the file has been sent will be displayed by the computer from which the control is maintained.

## 9.6. 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 if there is not enough space to store 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. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and open 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 24). You can use filter when searching for the object (see section 9.2, page 77).
3. Open the shortcut menu and use the **Delete** command or the analogous command under the **Action** menu.

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

## 9.7. 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** command or the analogous command under the **Action** menu.
3. In the **Backup Storage Properties** window that will open (see Figure 27) 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.

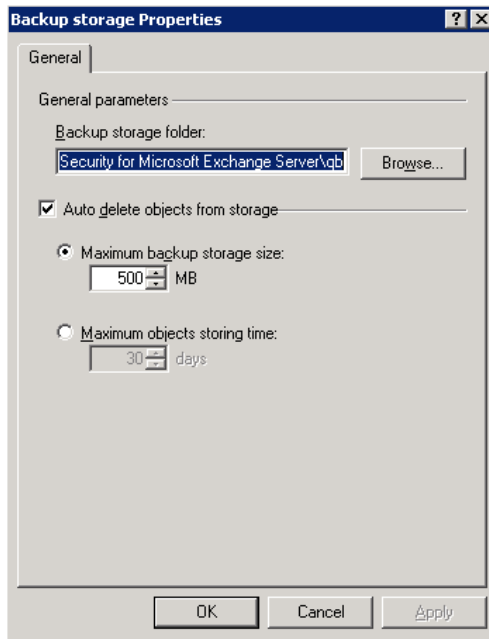


Figure 27. Configuring the backup storage settings

By default, the backup copy of the object is stored in **qb** folder. This is a service application folder, which is created in 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 in the folder where they had been placed initially. Objects from all folders are removed automatically based on the application restriction selected.



Please note that objects cannot be transferred from the old backup storage to the new backup directory!

To set a restriction on the size of the backup storage or on the time objects are stored in it, check the **Auto delete objects from storage** box, select one of the restriction options, and enter the desired value for the setting:

- **Maximum backup 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 500 MB). During the calculations, the total size of all objects is summed up no matter which folder a particular object is stored in.

- **Maximum objects storing time** – 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).

If the size of the backup storage does not need to be restricted, deselect the **Auto delete objects from storage** box.

In order to apply the changes, press the **Apply** or the **OK** buttons. To exit without saving the changes, press the **Cancel** button.

---

# CHAPTER 10. NOTIFICATIONS

Kaspersky Security allows notifying about revealed infected objects and about messages that contain SPAM.

Notifications can be delivered using the following methods:

- by sending e-mail messages;
- by sending messages using Net Send tools;
- by registering the event in the Microsoft Windows event 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 Microsoft Windows tool used for viewing and managing the logs.

There is a provision to notify the sender and the recipient of the message about the infected object or about blocking the message containing SPAM attributes.



No notifications are sent to the recipients of blind carbon copies (Bcc).

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 occurs, an 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 creating notifications for the administrator, sender, recipient and security services that vary as far as the content and the delivery method are concerned.

By default, notification template informing about found infected objects is generated during Security Server installation. Notification using this template is not issued. You can configure notification using this template as the basis.

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

The list of created notification templates is provided in the form of a table (see Figure 28). The table contains the name of the template, notification type and status for each template (enabled or disabled).

You can learn more about templates parameters in the settings window that opens by the **Properties** command available through the shortcut menu (details see section 10.2, page 91).

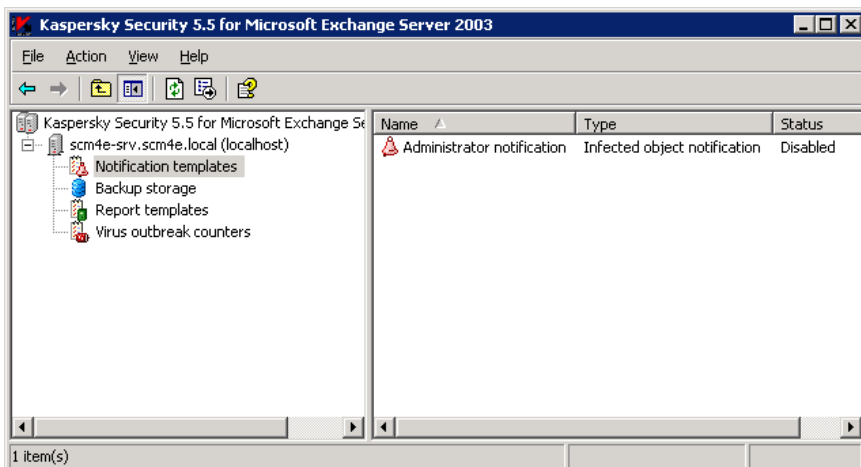


Figure 28. The **Notifications templates** folder

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 objects detected during scan.*

1. Create a notification template (see section 10.1, page 87) or select an existing template and configure its settings (see section 10.2, page 91).
2. Check the **Notify about event** box in the **General** tab of the notification template settings dialog box (see Figure 29).

## 10.1. 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>** window used for configuring new notification template will open (Figure 29). Specify the required values for the parameters in the tabs of the window.

Perform the following actions on the **General** tab (see Figure 29):

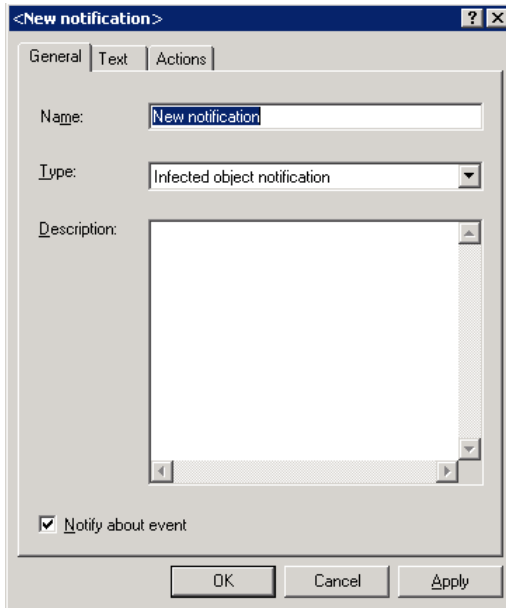


Figure 29. Notification template. The **General** tab

- 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 list.
- 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 30):

- Enter a brief description of the notification in the **Notification subject** field. This line will be used as a 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 list of macros will depend upon notification type). A description of the macros in the list is provided in Appendix A, page 160.

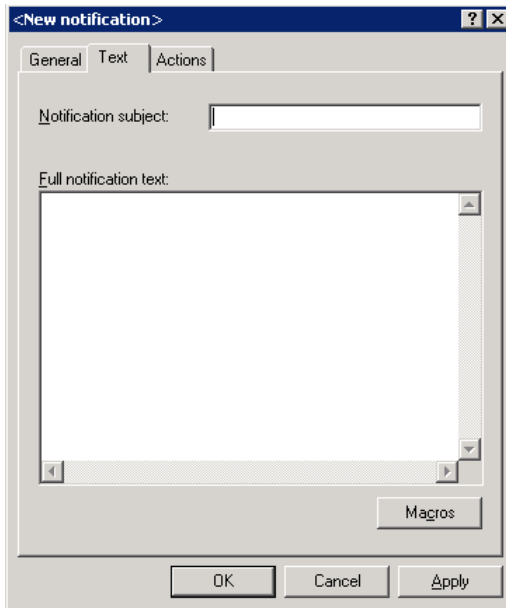


Figure 30. Notification template. The **Text** tab

Select the notification method and specify the corresponding parameter values in the **Actions** tab (see Figure 31). The application provides for several methods to be used.

- In order to send messages via the mail server, check the **Notify by e-mail** box and specify the recipients' addresses for the mailing.
  - In order to notify recipients and senders of the infected message about the event occurrence, 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.

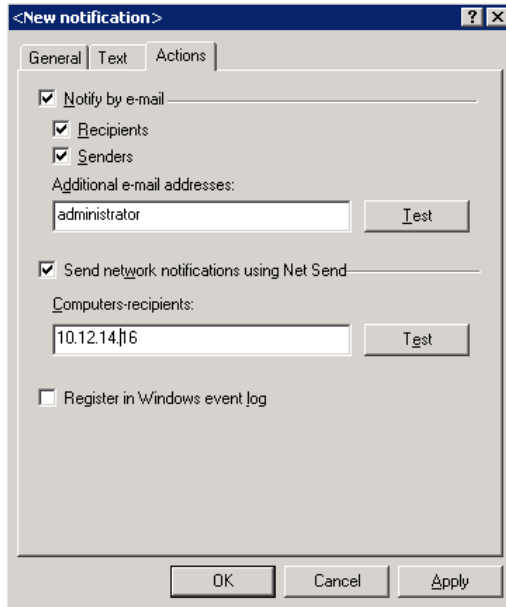


Figure 31. Notification template. The **Actions** tab

- 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-recipient in the **Computers-recipient** field  
IP address or NetBIOS-computer name can be used as the computer address. Entering several addresses is allowed, the addresses entered must be separated by semicolons.  
The validity of the addresses can be verified using the **Test** button. A message will be sent to the specified address.
- In order to register events in the Microsoft Windows system log, check the **Register in Windows event log** box.

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

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.

## 10.2. 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 28).
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>**. This window consists of the following tabs: **General**, **Text**, **Actions** and is completely similar to the **<New Notification>** window (see Figure 29). Parameters are changed in the same way they were specified when the notification was created (details see section 10.1, page 87).

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

## 10.3. Customizing general notification settings

When the application sends e-mail notifications, it places the **KSE** (Kaspersky Security for Microsoft Exchange Server) value in the **From** field by default. That may cause identification of such messages as formal spam. To resolve the problem, specify an existing SMTP address that will be used to send the notifications instead of **KSE**.



*You can modify the information, which will appear in the **From** field of sent e-mail notifications. In order to do this, perform the following actions:*

1. In the main application window, select in the console tree the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node, open it, select the node corresponding to the necessary server and use the [General settings](#) hyperlink in the results pane.

2. It will open the **General settings** window, where you should select the **Advanced** (see Figure 32) tab. Enter the information that will be displayed as the sender of messages generated by Kaspersky Security in the **From** field.

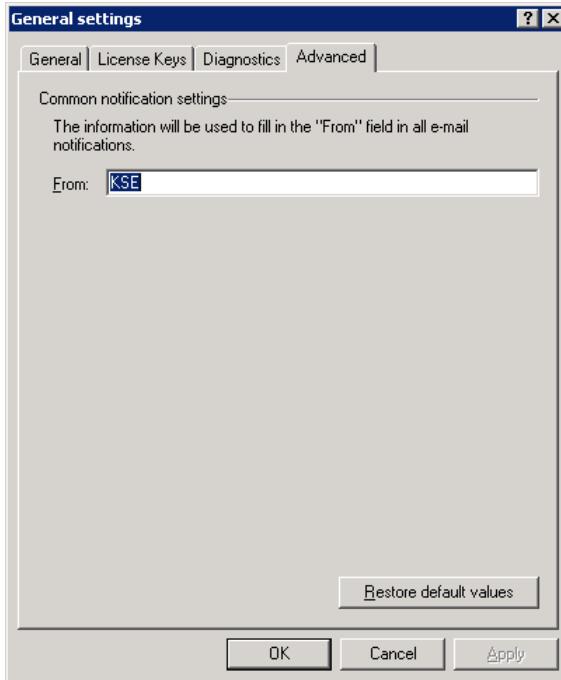


Figure 32. Configuring common notification settings

---

# CHAPTER 11. PREVENTING VIRUS OUTBREAKS

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 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 may be very useful in the periods of virus outbreaks as it helps the administrator to timely react to 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 corrupted 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 the following methods:

- by e-mail messages;
- by messages sent over the network using Net Send;
- by registering the event in the **Microsoft 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 Microsoft 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 outbreak 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 outbreak 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 any event.

During Security Server setup a virus outbreak counter is created. The counter can be used to set up a respective notification. By default, notifications about increased virus activity level are not issued.

Virus outbreak 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 outbreak counters created is displayed in the form of a table in the results pane (see Figure 33). The table displays the name, type and status (is notification about virus activity enabled or disabled) 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 section 11.2, page 99).

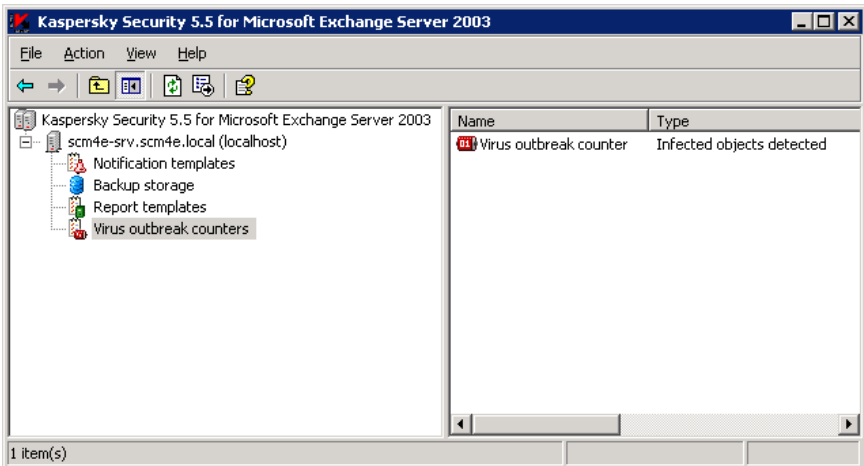


Figure 33. The **Virus outbreak counters** folder

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 section 11.1, page 95) or select an existing counter and configure its settings (see section 11.2, page 99).
2. Check the **Notify me about virus outbreaks** box in the **General** tab of the virus outbreak counter settings (see Figure 34).

## 11.1. 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** command 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 34). Specify the required values for the settings displayed in the tabs of this window.

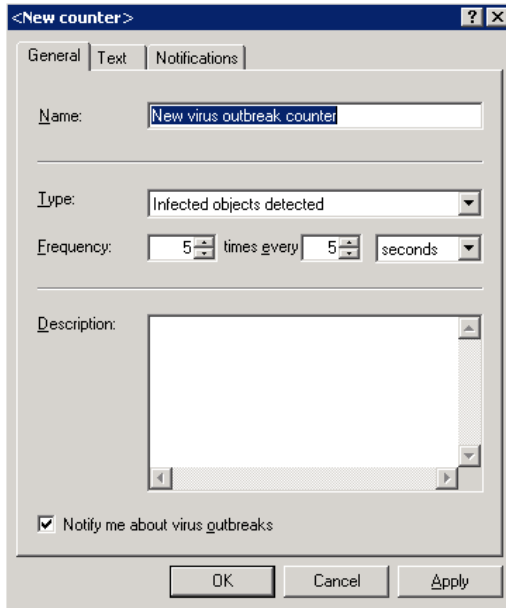


Figure 34. Virus outbreak counter. The **General** tab

Perform the following in the **General** tab (see Figure 34):

- 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.
- 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;
  - time unit **seconds, minutes, hours** or **days**.
- 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 35):

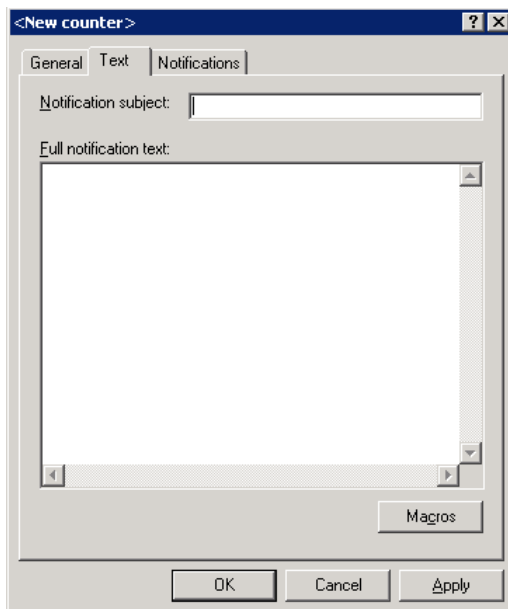


Figure 35. Virus outbreak counter. The **Text** tab

- Enter a brief description of the notification in the **Notification subject** field. This line will be used as a 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 160.

Select the notification method and specify the corresponding parameter values in the **Notifications** tab (see Figure 36). The application provides for several methods to be used.

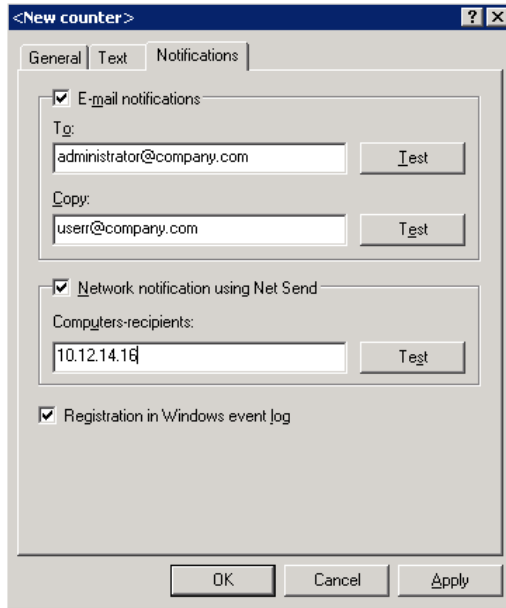


Figure 36. Virus outbreak counter. The **Notifications** tab

- In order to send messages via the e-mail server, check the **E-mail notifications** 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 notification 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. Entering several addresses is allowed, the addresses entered must be separated by semicolons.

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

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

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 in the table in the results pane;
- if the **Notify me 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.

## 11.2. Viewing and modifying virus outbreak notification settings



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

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the necessary server and 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 33).
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 counter settings window **<Counter name>: Properties** will open. This window includes the following tabs: **General, Text, Notifications** and is completely analogous to the **New counter** window (see Figure 34). Notification settings can be modified in the same way as they are specified when the notification is created (details see section 11.1, page 95).

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

---

# CHAPTER 12. REPORTS

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 allows receiving reports about the results of the anti-virus Exchange Server protection and about the anti-spam protection results.

Reports are generated automatically according to the schedule or manually by request and can be saved in a specified 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 section 12.2, page 108). This folder is created with the name that reflects the date and the time when the report was created in the following format **<report name: 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 section 12.1.2, page 107).

Reports sent by e-mail are files in HTML format sent by e-mail as attachments. The message contains clarification text as follows: *This message is created by Kaspersky Security 5.5 for Microsoft Exchange Server 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, during Security Server installation two in-built report templates are created - the anti-virus scan report and the anti-spam scan report. Based on these templates, the application generates reports on the first day of each month covering last 30 days. They are stored in the **Reports** subfolder of the application directory.

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 is displayed in the form of a table in the results pane (see Figure 37).

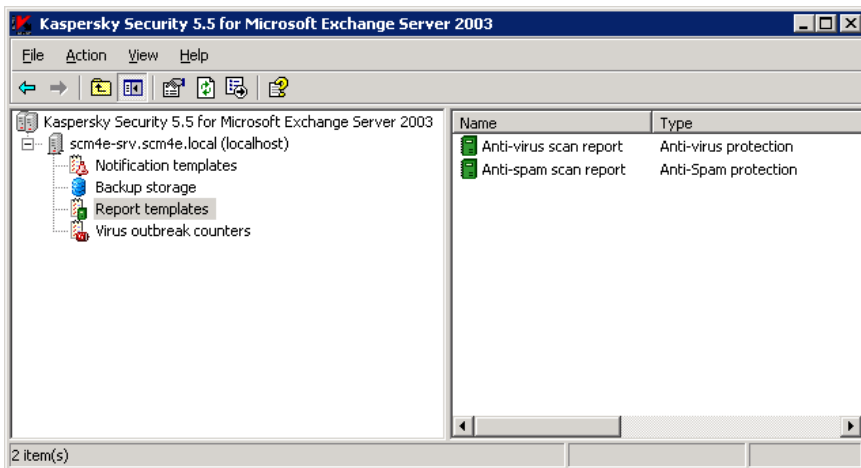


Figure 37. The **Report templates** folder

Apart from the reports' names, this table contains information on the status for each report created based on the template. Depending on the current stage of the report creation, its 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;
- **disabled** – report generation is disabled for this template.

Detailed information about report template settings is provided in the settings window accessible through the **Properties** shortcut menu command (details see section 12.1.2, page 107).

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

## 12.1. Receiving reports



*In order to receive a report about an anti-virus server scan or an anti-spam scan:*

1. Create a report template of an appropriate type (see section 12.1.1, page 104) or select an existing template and configure its settings (see section 12.1.2, page 107).
2. Check the **Create a report** box in the **General** tab of the report template settings window (see Figure 39).

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

In order to view the results of the scan, open the report for the corresponding reporting period (details see section 12.2, page 108).

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 status of server protection, for example, during virus outbreaks.



*In order to receive a report upon request:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the necessary server and 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 37).
3. Open the shortcut menu and use the **Create a report** command 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 a report** box in the **General** tab of the report template settings window (see Figure 39) is checked.*

Reports will be created based on the information about the anti-virus server scans and anti-spam scans results, saved by the application. The application saves all mail traffic scan results, transit mail scan 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 as well as the maximum number of lines per report section.



*In order to restrict the report storage period:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and select the **Report templates** folder in the console tree.
2. Open the shortcut menu and use the **Properties** command or the analogous command under the **Action** menu.
3. In the **Report templates Properties** window that will open (see Figure 38):

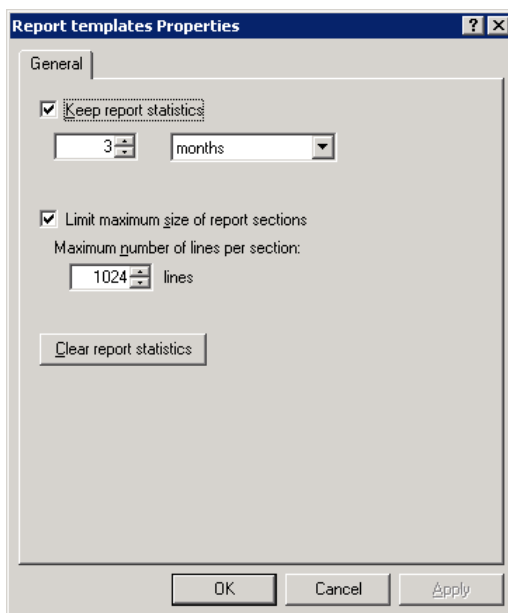


Figure 38. Configuring report settings

- Check the **Keep report statistics** box to limit the storage period for reports, then indicate the actual storage period and select the unit. The default storage period is three months.
- Check the **Limit maximum size of report sections** box to restrict the volume of data contained in a report. Then specify the maximum number of lines per single report section. The default limitation is 1024 lines per section.

- To delete contents of the statistical database on program operation used for creating reports, click **Clear report statistics** button.

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. To exit without saving the changes, press the **Cancel** button.

## 12.1.1. Creating a report template



*In order to create a new report template,*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and select the **Report templates** folder in the console tree.
2. Open the shortcut menu and use the **New template** command or the analogous command under the **Action** menu.
3. As a result, a report template settings window **New report** will open (see Figure 39); 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 39):

- Enter the template name in the **Name** field.
- Specify the report type: **Anti-virus protection** or **Anti-spam protection**;
- 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

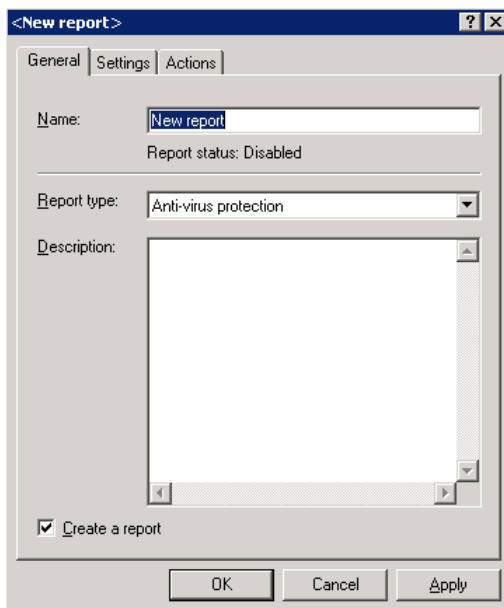


Figure 39. Report template. The **General** tab

Specify the reporting period and the report creation schedule settings in the **Settings** tab (see Figure 40).

- 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.

- Specify the time when reports will be created in the **Generate report at** field.

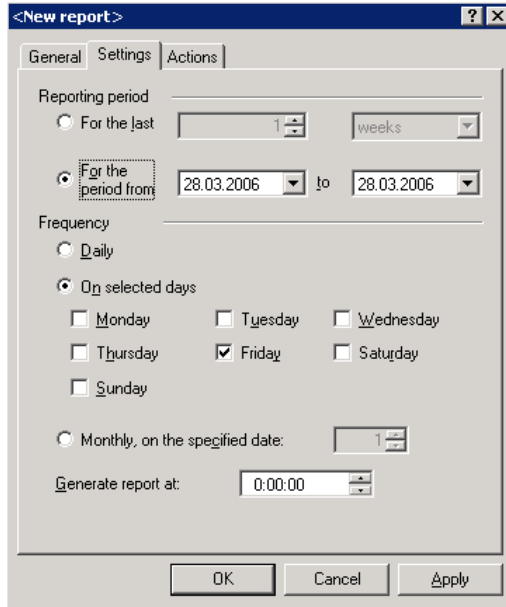


Figure 40. Report template. The **Settings** tab

Specify which format shall be used for reports to creation and specify the reports storage folder and mailing list in the **Actions** tab (see Figure 41).

- In order to create a report and save it in the server file system folder, check the **Save report** box.

Then, specify the folder where reports will be saved. By default, the **Reports** 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 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.

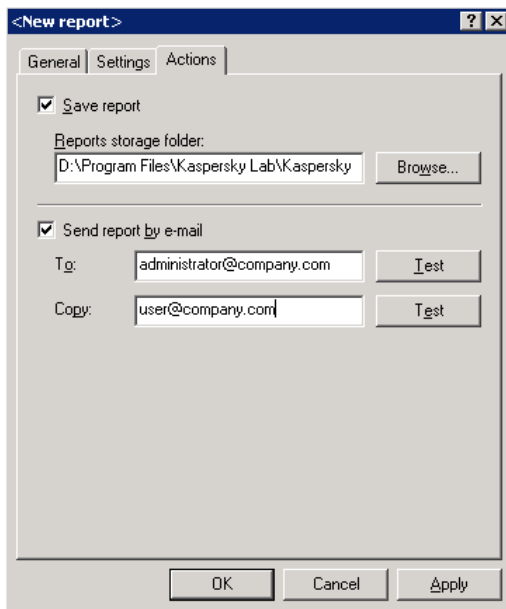


Figure 41. Report template. The **Actions** tab

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 in the table in the results pane;
- If the **Create a report** 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.

## 12.1.2. Viewing and fine-tuning 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 37).
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 report template settings window **<Template name>: Properties** will open.

This window includes the following tabs: **General**, **Parameters**, **Actions** and is completely analogous to the **New report** window (see Figure 39). Template settings can be modified in the same way as they are specified when the template is created (see section 12.1.1, page 104).

## 12.2. Viewing reports

Depending on the template settings assigned, created reports 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 as a folder,*

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 **<report name: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 results of server scanning for viruses or spam (depending upon the report type) will be displayed in the main window of the browser (see Figure 42). Immediately after loading, the report displays general results of the scan. The reporting period will be specified in the heading.

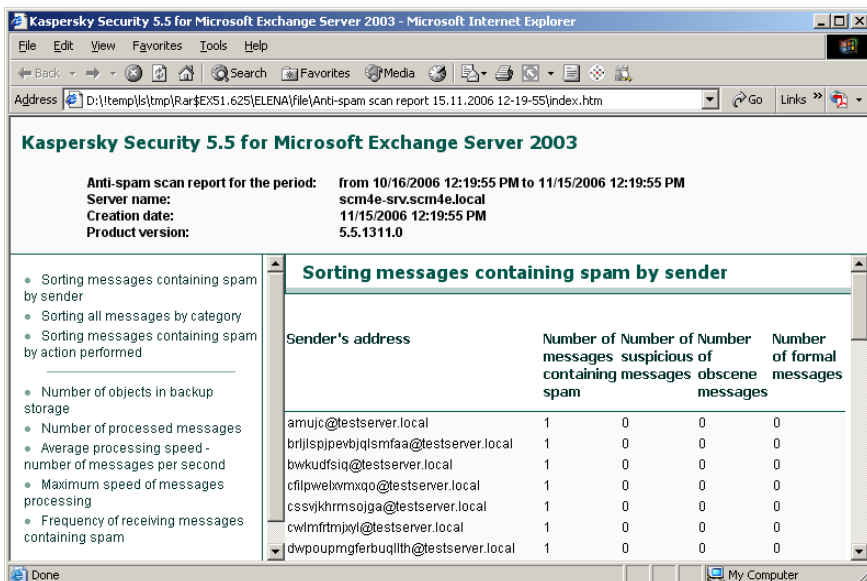


Figure 42. Viewing a report saved as a folder

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 its name in the table of contents and the content of the section will be loaded in the right frame.



*In order to view the 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 results of server scanning for viruses or spam (depending upon the report type) will be displayed in the main window of the browser (see Figure 43).

**Kaspersky Security 5.5 for Microsoft Exchange Server 2003**

**Anti-Virus scan report:** from 10/16/2006 12:19:56 PM to 11/15/2006 12:19:56 PM  
**Server name:** scm4e-srv.scm4e.local  
**Creation date:** 11/15/2006 12:19:56 PM  
**Product version:** 5.5.1311.0

- [General scan results](#)
- [Malicious objects detected](#)
- [Senders of infected objects](#)

---

- [Number of objects processed](#)
- [Average object processing rate](#)
- [Maximum object processing rate](#)
- [The rate of receiving infected objects](#)

**General scan results**

Object status	Number of objects
not infected	2
suspicious	50
failed to be disinfected	100

**Malicious objects detected**

Malicious object name	Detected
EICAR-Test-File	100

**Senders of infected objects**

Sender address	Number of malicious objects
----------------	-----------------------------

Figure 43. Viewing a report delivered by e-mail

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.

---

# CHAPTER 13. APPLICATION'S EVENT LOGS

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 allows the user to perform full diagnostics of its operation and register events in the Microsoft Windows event log and in the Kaspersky Security application's log file.

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 section 13.1, page 112).

Events registered in the Microsoft Windows event log can be viewed using standard Microsoft Windows tool – **Events Viewer**. For Kaspersky Security the **Source** column will contain **KSE** line.



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

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 event 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 event log where information pertaining to anti-virus protection is appended.

*kscmasDATE.log* – main application's event log where information pertaining to anti-spam server protection is appended.

*FILENAME.rawDATE.log* – a log that contains unformatted data pertaining to the activity of individual application components if, for some reason, it could not be entered in the main log. FILENAME part corresponds to the name of the component writing the 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, a new file will be created with a postfix added to the filename. For example, *kavscmesrv20040410\_1.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 number 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 section 13.2, page 114).

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

The application logs can be viewed using a standard program associated with text files (e.g., notepad.exe).

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 section 13.2, page 114).

Logs' settings can be modified in the **Diagnostics** tab of the application settings window **General settings** (see Figure 44). This window is accessible via the [General settings](#) link.

## 13.1. 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.

The following diagnostics levels are provided:

- **None** – do not register any information in the logs.
- **Minimum** – log only major events.
- **Medium** – in addition to major events, log some additional events that describe the application's 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 settings](#) link in the results pane.

2. Go to the **Diagnostics** tab in the **General settings** window that will open (see Figure 44).

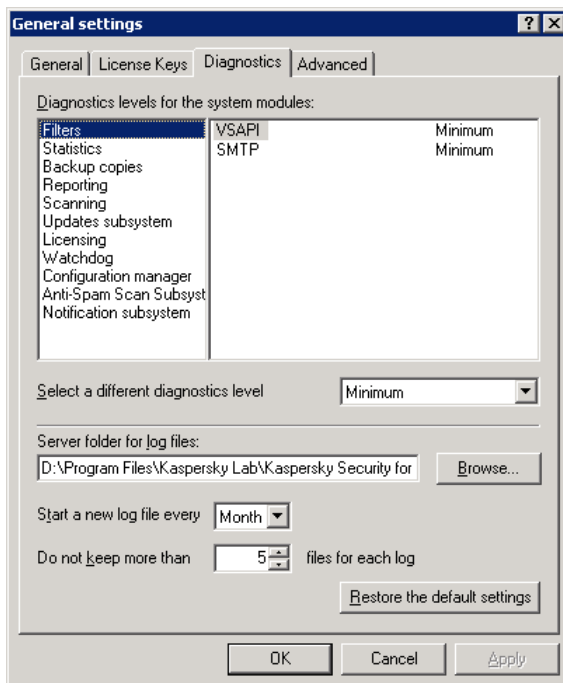


Figure 44. The **Diagnostics** tab

The **Diagnostics level for the 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 component.

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 levels for each module.

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.

## 13.2. Configuring log settings



*In order to configure log settings:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [General settings](#) link in the results pane.
2. Go to the **Diagnostics** tab in the **General settings** window that will open (see Figure 44).
  - Enter the path to the new folder in the **Server folder for log files** field.
  - Select the frequency for creating logs in the **Start a new log file every** field by selecting the required value from the drop-down list.
  - 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.

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 14. LICENSE KEYS

When you purchase Kaspersky Security 5.5 for Microsoft Exchange Server 2003, you enter into a license agreement with Kaspersky Lab. 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 mailboxes.



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;
- using the anti-spam functionality of the application;
- *regular* anti-virus database and content filtration database updates;
- 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 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 Security 5.5 for Microsoft Exchange Server 2003 WILL NOT WORK without a license key!**

The application can use **only one** active license key. This license key contains restrictions imposed on the use of Kaspersky Security that can be verified by the special application's components. If any violation of the terms and conditions of the license agreement has been detected:

- the functionality of the application will be limited;
- a record about the violation detected will be entered into the event logs;
- if the notification settings are configured, a notification of the violation will be issued and sent by e-mail (details see section 14.4, page 121).



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 section 12.2, page 108). We recommend that you start a background scan after the functionality of the application is restored (after the new license key is installed) to scan these objects (see section 6.6, page 62).

You can change the number of protected mailboxes by excluding some of them from the storage scan scope; such mailboxes will not be scanned (details see section 14.5, page 122).

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. In order to receive the notification, specify the e-mail address to which it should be sent (see section 14.5, page 122).

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 the application will be preserved except for the possibility to update its databases. The application will continue to perform anti-virus traffic scan, background storages scan and the anti-spam scan of the incoming mail, but it will use outdated versions of the anti-virus and content filtration databases. In this case, it is difficult to guarantee comprehensive anti-virus protection against new viruses and new types of spam that appeared after license expiration.

By default, a notification is sent 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, as well as information about extending a license. You can change the date of the notification and specify an e-mail address to which the notification should be sent (see section 14.4, page 121).

We recommend that you timely renew your application's license.



*In order to renew your license you have to purchase and install a new license key for your Kaspersky Security 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 Security 5.5 for Microsoft Exchange Server 2003.

or

Purchase a new license key directly from Kaspersky Lab. To do so, click the [License renewal](#) link in the **License Keys** window (see

Figure 46). If you have trial license key installed, click [Buy license](#). This will send you to the Kaspersky Lab website, where you will find complete information on buying or extending a license.

2. Install the license key (see section 14.2, 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 Lab 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.

In case if you find that your key is in the "black list", you are advised to update your databases and, if the error persists, contact the Technical Support.

## 14.1. License information



*In order to view the license:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select the node corresponding to the server you need and follow the [General settings](#) link in the results pane.
2. Go to the **General** tab in the **General settings** window that will open (see Figure 45).

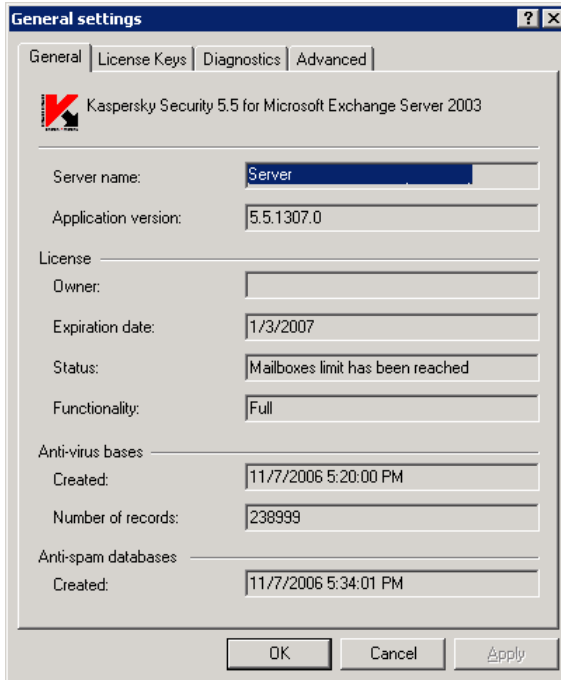


Figure 45. Viewing license information

The tab contains the following information:

- the name of Exchange server where the Security Server component is installed;
- the version (number) of the application installed;
- license owner information;
- license expiration 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 updating feature for anti-virus and content filtration databases is not available. The application performs scanning for viruses and spam using

- outdated versions of its databases. Your license may be expired.
- **Management services only.** Only management services used to configure the application parameters (license key installation) are available. This may be caused by the expiration of the trial license key.
  - **Update only.** Only database updating feature is available. The databases may have been corrupted; therefore, the e-mail scanning cannot be performed. In this situation, we recommend that you update the databases and, if the error has not been eliminated, contact the technical support service.
- the status of anti-virus and content filtration databases.

## 14.2. 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.



A backup key cannot be installed if its validity expires earlier than the same period of the current license key!

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



*In order to install or to replace the license key:*

1. In the main application window select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** node in the console tree, open it, select node corresponding to the required server in the console tree and follow the [General settings](#) link in the results pane.
2. Go to the **License Keys** tab in the **General settings** window that will open (see Figure 46).

- 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 key...** in the **Backup license key** section.

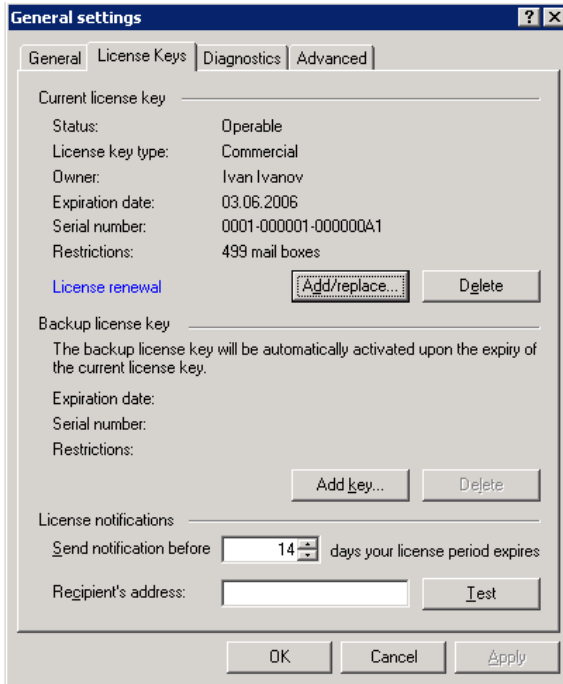


Figure 46. View license key info.  
Configuring license notifications

3. 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.

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

## 14.3. Removing a license key

When you remove your license key using the Kaspersky Security interface, only the registration of the key with the application will be removed. Physically, the key will remain on the media from which it had been added to the application.



*In order to remove a license key,*

1. Select the node corresponding to the required server in the console tree and follow the [General settings](#) link in the results pane.
2. Go to the **License keys** tab in the **General settings** window that will open (see Figure 46).
  - if you are removing the backup license key, press the **Delete** button in the **Backup license key** section.
  - if you are removing the current license key, press the **Delete** button in the **Current license key** section.
3. 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.

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



**If you remove the current license key, any installed backup key will also be automatically removed.**

## 14.4. 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 and the content filtration 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 to the specified e-mail address.

By default, a notification will be issued 14 days before your license period expires. 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 settings](#) link in the results pane.
2. Go to the **License keys** tab in the **General settings** window that will open (see Figure 46).

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.

In order to check this e-mail address, send an e-mail message to it by pressing the **Test** button.

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

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

## 14.5. Unprotected storage areas

The application is designed to ensure protection of the number of mailboxes 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 moved into the storage areas not covered by the anti-virus protection. If the version of Exchange Server installed on your computer supports only one storage, you will have to purchase a license that covers protection of all mailboxes of this area.

By default, all public folders created on a protected mail server, are covered by the protection. You can remove protection from public folders if you think that their scan would be redundant.



*In order to remove protection from 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 13) tab in the **Anti-virus protection** window that will open.

- Uncheck boxes next to the names of storage areas in the **Protected mailbox storages** 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.

- Uncheck boxes next to the names of public folders in the **Protected public folders storages** 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.

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.



Please note that after modifications of the list of protected areas or public folders the application takes some time (approximately 15 minutes) to apply the new settings. In order to apply new settings immediately, you are advised to restart the anti-virus protection manually (see section 6.2, page 51).

---

# CHAPTER 15. APPLICATION MANAGEMENT USING KASPERSKY ADMINISTRATION KIT

**Kaspersky Administration Kit** is a centralized system performing the main administration tasks pertaining to the management of corporate network security system built on the basis of applications included into the bundles of Kaspersky Anti-Virus Business Optimal or Kaspersky Corporate Suite.

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 is a product of Kaspersky Lab, which can be managed both using its own interface (the method is described above in this guide) or via Kaspersky Administration Kit (if the computer acts as a part of a centralized remote management system).

There are two possible approaches to application management via the interface of Kaspersky Administration Kit:

- **Local management** – install the following programs on the computer running Microsoft Exchange Server: Kaspersky Security 5.5 for Microsoft Exchange Server 2003, *Network Agent* and *Administration Console* included into the package of Kaspersky Administration Kit. In this case the application will be managed locally using the *Administration Console*.



If you are planning to control the application remotely using Kaspersky Administration Kit, then while installing the *Network Agent* make sure that the address (name and port) of the *Administration Server* is specified.

In case of local management using *Administration Console* you will be working with the **Local computer** object found in the Console tree only (see Figure 47).

In this mode you can control the tasks and settings of Kaspersky Security installed on that particular server.

- **Remote management:**
  - Install the following programs on the computer running Microsoft Exchange Server: Kaspersky Security 5.5 for Microsoft Exchange Server 2003 and *Network Agent* (included into Kaspersky Administration Kit).

- Deploy the *Administration Server* in the network; install *Administration Console* to the administrator's workplace (please refer to the administrator's guide for "Kaspersky Administration Kit" for details).

You can manage the application using Kaspersky Administration Kit via its Administration Console (see Figure 47). It is a standard **MMC snap-in**, which allows the administrator to perform the following operations:

- Remotely install the *Network Agent* on a computer with Microsoft Exchange Server 2003;
- Remotely configure Kaspersky Security 5.5 for Microsoft Exchange Server 2003;
- Update the anti-virus and content filtration databases;
- Install and remove license keys on client computers;
- Review information about application activity on client computers.

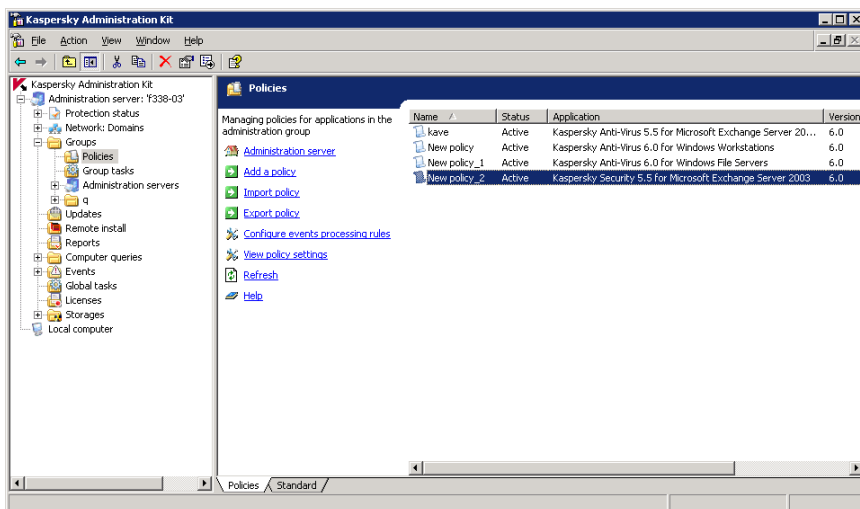


Figure 47. Kaspersky Administration Kit Console

When working through Kaspersky Administration Kit, the program is administered by policy settings, task settings, and application settings set by the administrator.

A **task** is a specified action performed by the application. The tasks are subdivided in accordance with their purpose (the task for updating the anti-virus and content filtration databases, the task for license key installation). Each task has a set of parameters specified to control its execution, i.e. *task settings*.

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

A distinctive feature of the centralized administration is the arrangement of computers into groups and modification of their settings by creating and defining group policies.

A **policy** is a set of parameters for the functioning of the application on computers in network workgroups and also a set of restrictions for redefining those parameters during application or task setup on individual client computers.

A policy includes all required parameters for executing each of the application features, and includes both application settings and settings for all task types, except for parameters specific to a certain task type.

## 15.1. Managing policies

This section describes how to create and manage policies of Kaspersky Security 5.5 for Microsoft Exchange Server 2003. Detailed information about managing policies is available in the administrator's manual for Kaspersky Administration Kit.

### 15.1.1. Creating a policy



*To create a new policy, perform the following actions:*

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

The program for creating a new policy is organized as a Microsoft Windows Wizard, which will guide you through the process. To navigate between the wizard dialogs, use **Back** and **Next** buttons. To complete working with the wizard, click **Finish**. To close the wizard at any stage, click **Cancel**.



*When creating the policy, you can lock settings from being edited in policies for nested groups, application settings, and task settings.*

## Step 1. General information about the policy

The first wizard dialog boxes are introductory steps, where you should enter the policy name into the **Name** field and select the **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** product from the **Application** drop-down list. Enable the **Activate policy** checkbox to enforce it immediately after creation.



An application can only have one active group policy.

If there is an upper level group policy for the program, you can redefine only those settings in the created group policy that are allowed to be changed by the top level policy.

## Step 2. Enabling server protection

In the **Server protection** dialog (see Figure 48) you will be offered to define the necessary level of anti-virus protection (for details see section 6.1, page 49), and server protection against unwanted e-mail.

## Step 3. Configuring attachment scanning parameters

In the **Scanning of attachments** dialog (see Figure 49) you can restrict the list of attached objects, which the application will scan. Configuration of these parameters is similar to the case of application management via its local interface (for details see section 6.3, page 53).

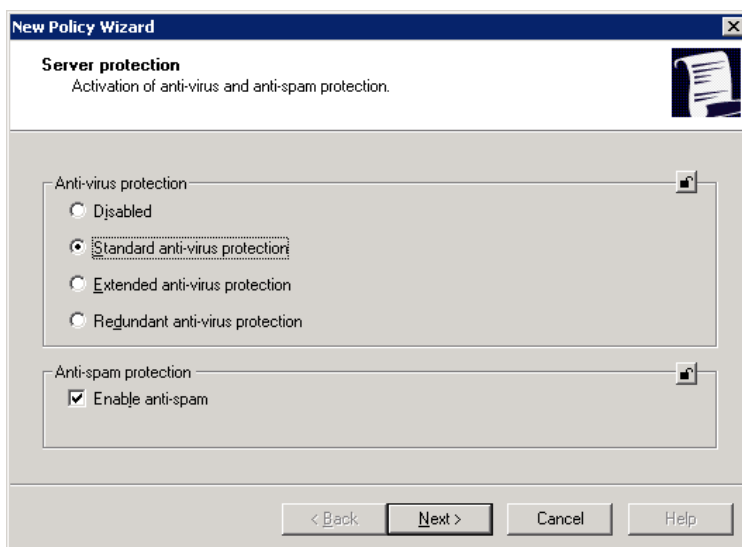


Figure 48. Enabling server protection

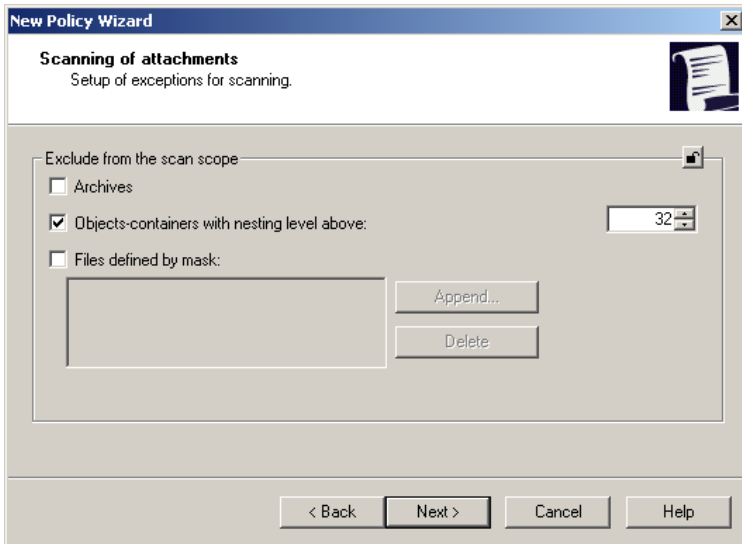


Figure 49. Scanning of attachments

#### Step 4. Enabling scanning of routed mail

You can use the **Protected e-mail** dialog (see Figure 50) to disable scanning of mail routed by the server in order to decrease the load on the Exchange server (see section 6.4, page 56).

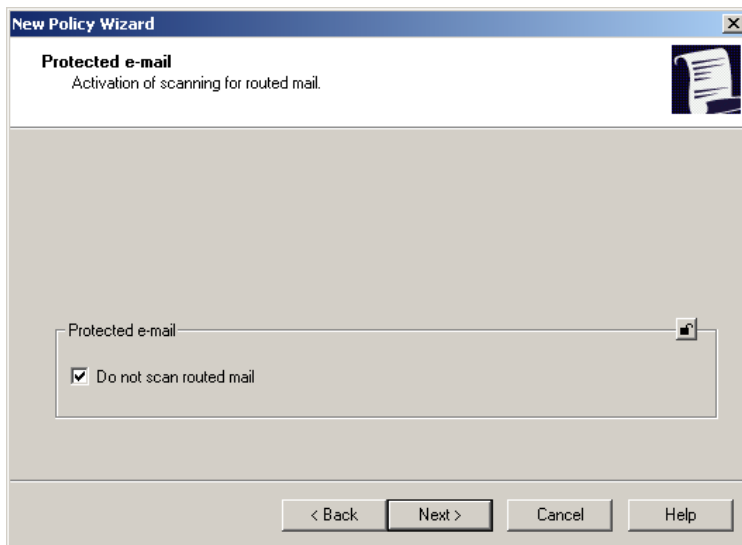


Figure 50. Scanning of routed mail

## Step 5. Selecting the source of updates

At this stage (see Figure 51), you are asked to configure the settings for anti-virus database and content filtration database updates:

- specify the update source (see section 5.3, page 41);
- configure local network settings in the window that opens when you click the **Connection parameters** button (see section 5.4, page 43);
- configure settings for running updates under another user account in the window that opens when you click the **Start parameters** button (see section 5.5, page 45).

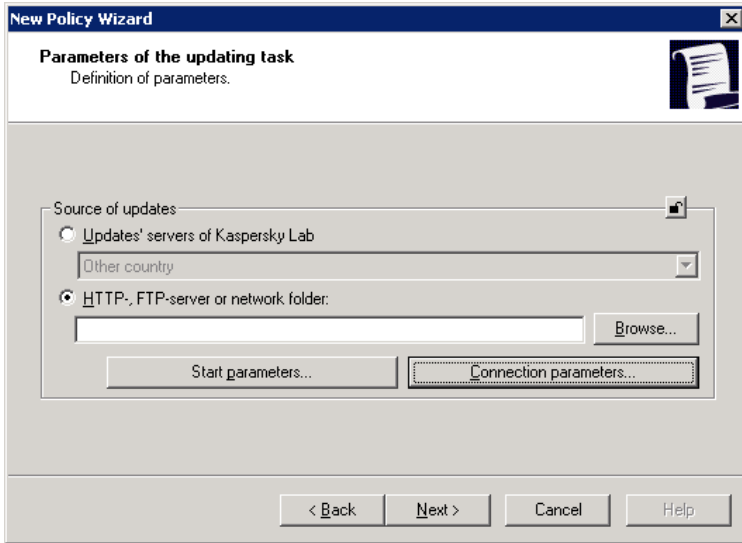


Figure 51. Selecting the update source

## Step 6. Finalizing policy creation

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

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

You can copy and move policies from one group to another and handle the policies using the standard commands in the shortcut menu, such as **Copy/Paste**, **Cut/Paste**, and **Delete**, or identical commands in the **Action** menu.

## 15.1.2. Viewing and editing policy settings

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

1. In the **Groups** folder of the console tree, select a group of computers for which you want to change policy settings.
2. Select the **Policies** folder in this group. All policies available for the group will be displayed on the results panel.

3. In the list of policies, point to a policy for **Kaspersky Security 5.5 for Microsoft Exchange Server 2003** (the application name is displayed in the **Application** field).
4. Open the shortcut menu for the selected policy and click **Properties**. You will see a window with the policy properties for **Kaspersky Security 5.5 for Microsoft Exchange Server 2003**, consisting of several tabs.

**General**, **Enforcement**, and **Event processing** tabs are standard Kaspersky Administration Kit tabs (see details in Administrator's manual for Kaspersky Administration Kit).

The remaining tabs display specific settings for Kaspersky Security 5.5 for Microsoft Exchange Server 2003. These tabs are described in detail further.

### **15.1.2.1. Viewing information about the application**

The **General** tab (see Figure 52) displays the general information about the policy:

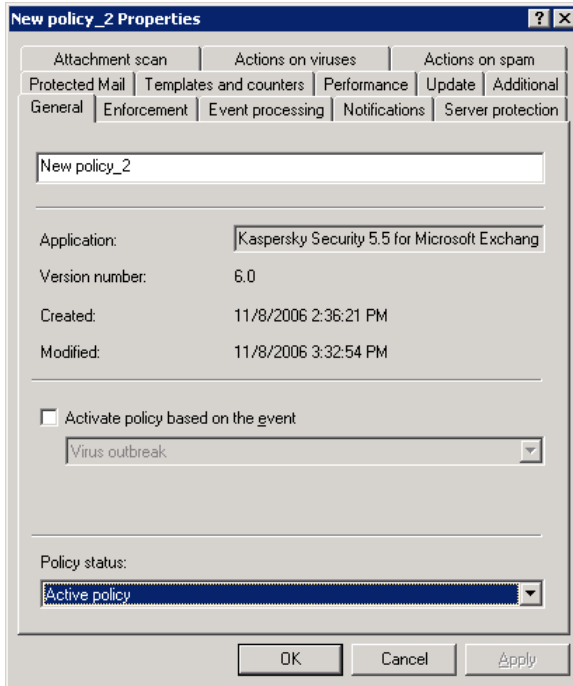


Figure 52. The **General** tab

- Policy name;
- The application this policy is assigned to (**Kaspersky Security 5.5 for Microsoft Exchange Server 2003**);
- Application version (number);
- Date and time of policy creation;
- Date and time of the last policy modification.

On this tab, you can edit the policy name, enable or disable it or define its activation whenever specified events occur.

### 15.1.2.2. Enabling / disabling server protection

You can use the **Server protection** tab (see Figure 53) to enable / disable anti-virus protection of the server and protection against unwanted e-mail for a group of client computers. In addition, you can specify TCP/IP parameters used during spam checks.

Upon enabling of the anti-virus protection you will have to select one of three available levels of anti-virus protection: **Standard**, **Extended** or **Redundant** (see section 6.1, page 49).

To enable anti-virus scanning of e-mail and contents of public folders stored on the server, check **Enable background scan** and configure the scan settings (for more on background scanning, see section 6.6, page 62).

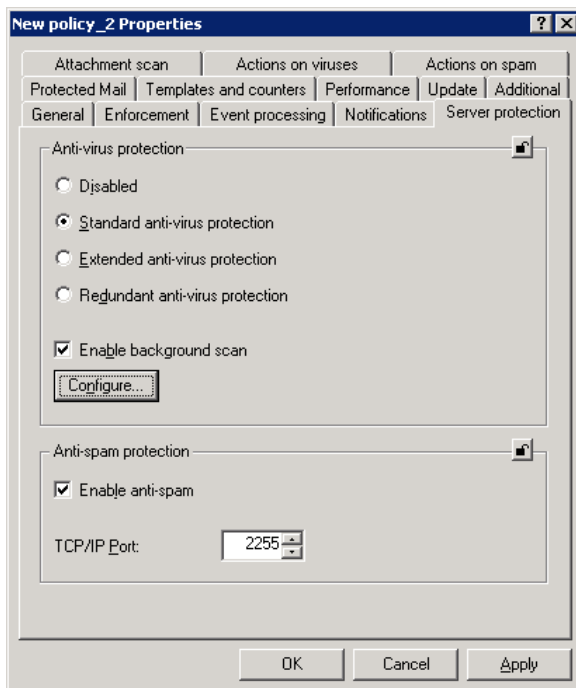


Figure 53. The **Server protection** tab

### 15.1.2.3. Scanning of attachments

You can use the **Attachment scan** tab (see Figure 54) to define the policy parameters that limit anti-virus scanning of attached objects. Configuration of these parameters is similar to the case of application management via its local interface (see details in section 6.3, page 53).

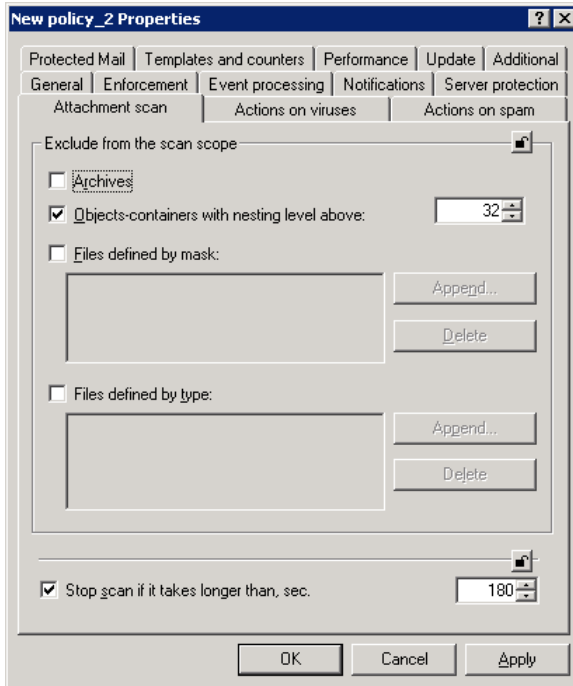


Figure 54. The **Attachment scan** tab

### 15.1.2.4. Scanning of routed mail

You can use the **Protected Mail** tab (see Figure 55) to enable / disable scanning of mail traffic routed via an Exchange server. Configuration of these parameters is similar to the case of application management via its local interface (see details in section 6.4, page 56).

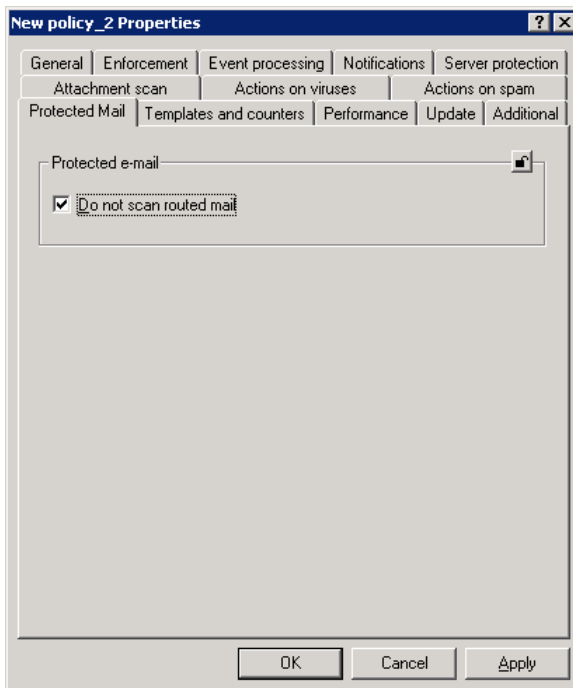


Figure 55. The **Protected Mail** tab

### 15.1.2.5. The choice of actions over objects

You can use the **Actions on viruses** tab (see Figure 56) to define the actions, which the Kaspersky Security application will perform whenever it reveals objects containing malicious code. In addition, you can enable the option to create a copy of the original object in the Backup storage prior to its disinfection.

Configuration of these parameters is similar to the case of application management via its local interface (see details in section 6.5, page 57).

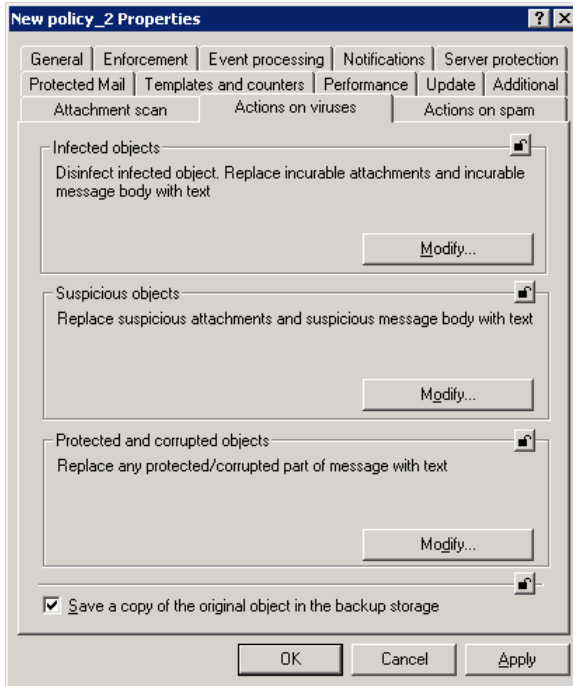


Figure 56. The **Actions on viruses** tab

### 15.1.2.6. The choice of actions over spam messages

You can use the **Actions on spam** tab (see Figure 57) to define the actions, which the Kaspersky Security application will perform whenever it detects messages bearing signs of spam, and also to configure special markers for flagging the subject line of the message. In addition, you can enable the option to create a copy of the original message in the Backup storage prior to its deletion or rejection.

Configuration of these parameters is similar to the case of application management via its local interface (see details in section 7.2, page 67).

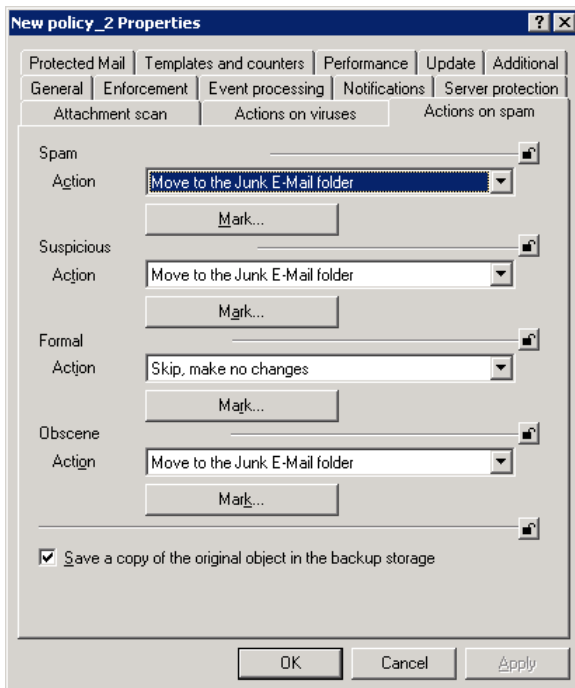


Figure 57. The Actions on spam tab

### 15.1.2.7. Configuring the server protection productivity

Anti-Virus and Anti-Spam productivity settings are configured on the **Performance** tab (see Figure 58).

These settings are configured in the same way as when configuring them through the application's own interface. For more, see Chapter 8, page 72.

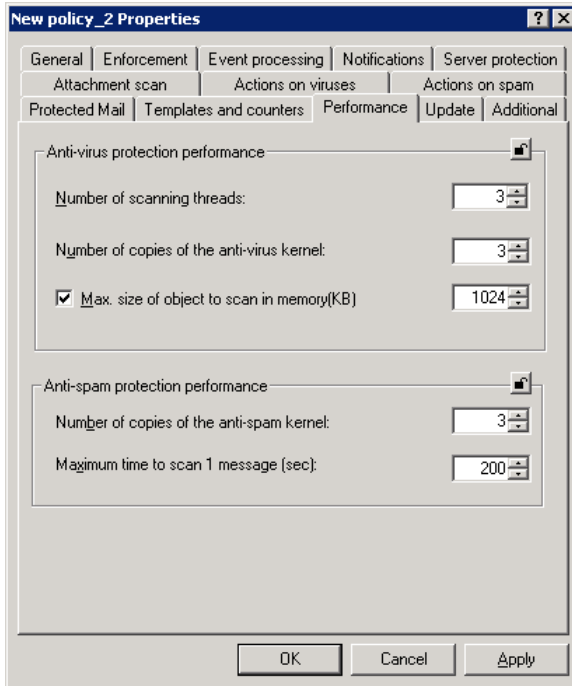


Figure 58. The **Performance** tab

### 15.1.2.8. Updating the anti-virus and content filtration databases

You can use the **Update** tab (see Figure 59) to define the policy parameters for updating of the anti-virus and content filtration databases. You will be offered to specify the source of updates and configure the local network parameters in the window, which opens after clicking the **Connection parameters...** button, and configure settings for running updates under a different user account. Configuration of these parameters is similar to the case of application management via its local interface (see details in sections 5.3–5.5, pages 41–45).

You can configure scheduled updates to update anti-virus and content filtration databases centrally for a group of computers that belong to a policy.

To do so, select an update mode (manually or scheduled) in the **Schedule** section. If you choose to use a schedule, assign the update interval.

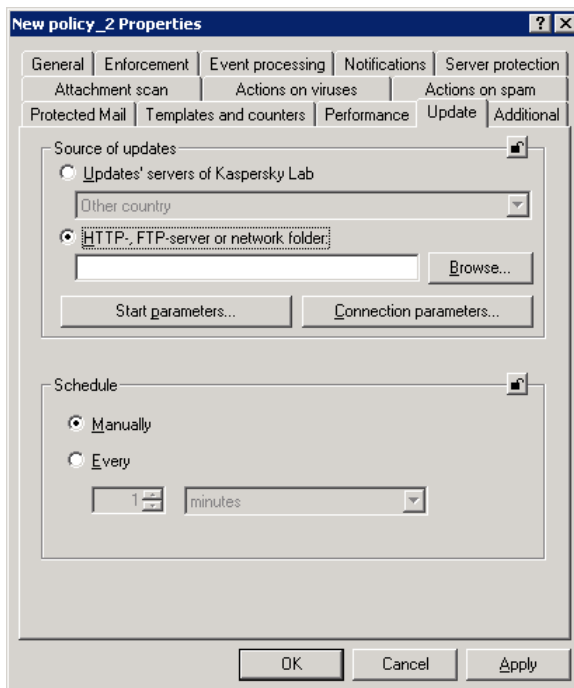


Figure 59. The Update tab

### 15.1.2.9. Notifications on detected objects

On the **Templates and counters** tab (see Figure 60), you can create notification templates for notifying the administrator or users when certain events occur in program operation.

In order to create a new template, click the **Append...** button in the **Notification templates** section and use the resulting window to configure the notification template. Configuration of these parameters is similar to the case of application management via its local interface (see details in section 10.1, page 87).

As soon as a new template is created, it will appear in the list of notification templates (see Figure 60). Click the **Properties** button to review/edit its parameters. To remove a template, click the **Delete** button.

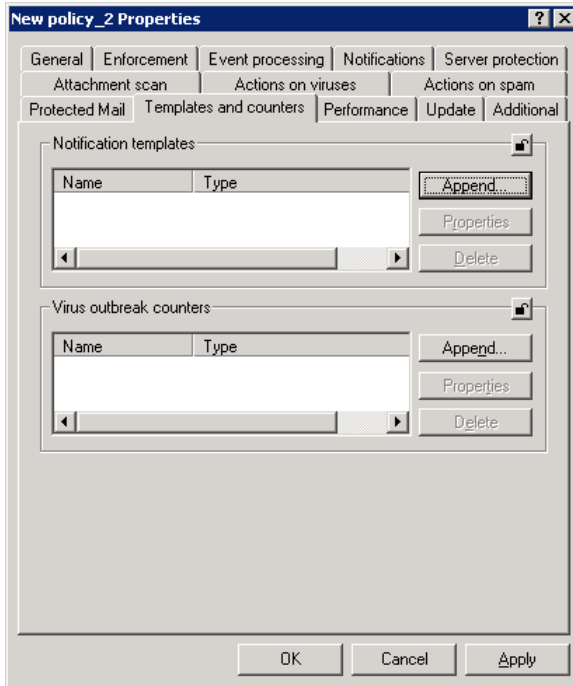


Figure 60. The **Templates and counters** tab

### 15.1.2.10. Virus outbreak notification

On the **Templates and counters** tab (see Figure 60) you can configure notification settings for virus activity.

In order to create a new counter, click the **Append...** button in the **Virus outbreak counters** section and use the resulting window to configure the counter. Configuration of these parameters is similar to the case of application management via its local interface (see details in section 11.1, page 95).

As soon as a new counter is created, it will appear in the list of **Virus outbreak counters**. Click the **Properties** button to review/edit its parameters. To remove a counter, click the **Delete**.

### 15.1.2.11. General notification settings

On the **Notifications** tab (see Figure 62) settings are configured for notifying the administrator or users of the expiration date for the program license. These

settings are configured in the same way as when configuring them through the application's own interface. For more, see section 14.4, page 121.

In addition, you can define whose account will be used when sending notifications by e-mail. By default notifications are sent under **KSE** (see section 10.3, page 91).

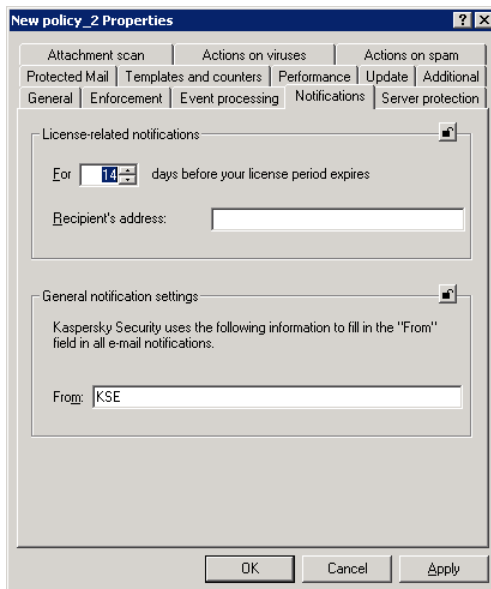
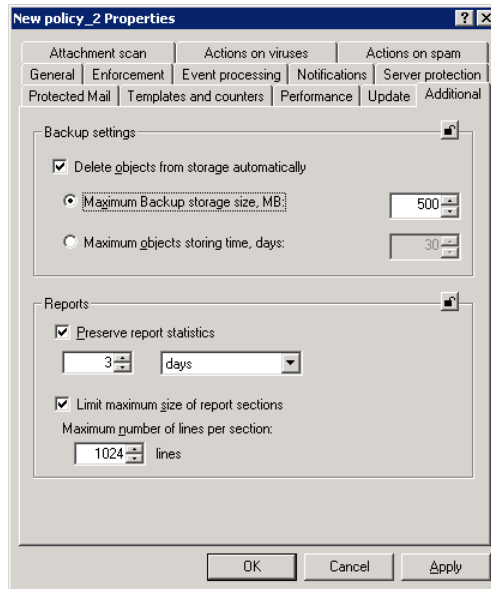


Figure 61. The **Notifications** tab

### 15.1.2.12. Additional settings

On the **Additional** tab (see Figure 62), you can configure Backup settings (for more, see section 9.7, page 83) and settings for saving report statistics (see section 12.1, page 102).

Figure 62. The **Additional** tab

### 15.1.2.13. Registration of events on program operation on Administration Server

On the **Event processing** tab (see Figure 63) you can configure settings for recording events that occur in program operation, on Kaspersky Administration Kit Administration Server, and the event notification mode for the administrator or users.

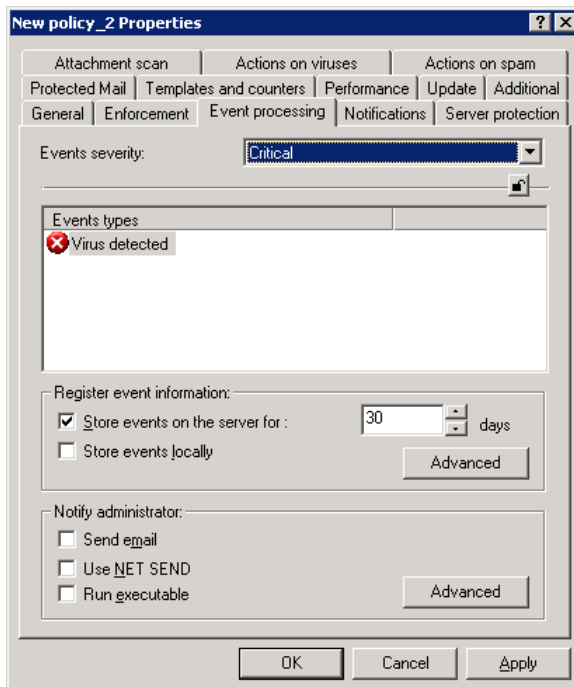


Figure 63. The **Event processing** tab

While running, the application generates a specific set of events. Every event is characterized by the level of its importance. There are four such levels:

- **Critical event**
- **Functional failure**
- **Warning**
- **Informational message**

Events of the same type may have various importance levels depending upon the situation in which they occur.

Use the **Events severity** drop-down list to specify the importance level for logged events. The list below displays the types of events corresponding to the selected level.

For each event you can define if it should be sent to the Administration Server, and you can configure settings for notifying the administrator of events that occur.

Please refer to the administrator's guide for Kaspersky Administration Kit for a detailed description of the **Event processing** tab.

### 15.1.2.14. Reviewing the results of policy application

The **Enforcement** tab (see Figure 64) displays the following information about the policy applied to the computers in the selected group:

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

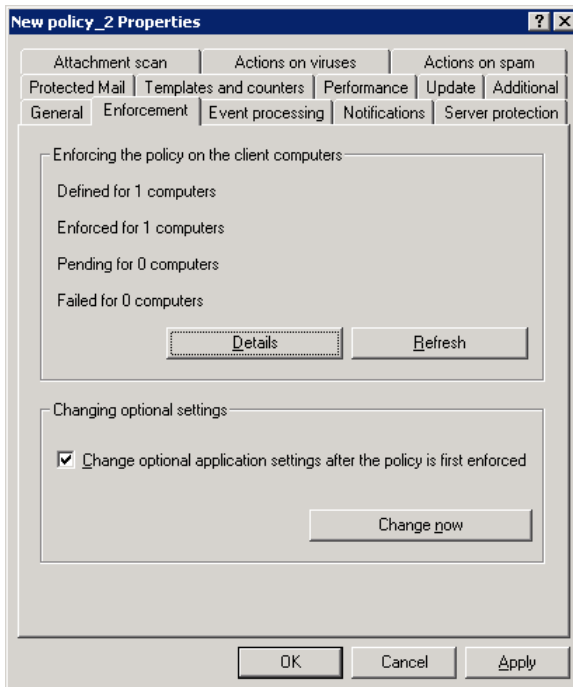


Figure 64. The **Enforcement** tab

Click **Details** to open a dialog box containing detailed information about the selected policy applied to each client computer (for details, see the administrator's guide for Kaspersky Administration Kit).

In addition, you can configure the procedure for modifying local application settings on client computers (for more, see the Kaspersky Administration Kit Administrator's Handbook).

## 15.2. Management of application settings

You can use application settings to modify the parameters of Kaspersky Security operation on individual client computers within a group or on a local computer running the application. Only parameters allowed for modification in the corresponding application policy can be changed (see details in section 15.1, page 126).



*In order to modify the application settings,*

1. In the **Groups** folder of the console tree, select the folder containing the required client computer.
2. In the results pane, select the computer where the application settings have to be modified, and use the **Properties** command from the right-click menu or an identical option from the **Action** menu.



To configure the application parameters on the local computer, select the **Local computer** object (see Figure 47) in the console tree and use the **Properties** command from the context menu.

3. Doing so will open a **<Computer name> Properties** dialog in the main program window. Select the **Applications** tab (see Figure 65). It contains a complete list of Kaspersky Lab applications installed on the client computer.
4. Select **Kaspersky Security 5.5 for Microsoft Exchange Server 2003**. You can use the buttons below the list (**Events**, **Statistics**, **Properties**) to:
  - Review the list of application events, which have occurred while the client computer was running, registered at the Administration server (please refer to the administrator's guide

for Kaspersky Administration Kit for details on work with reports).

- Review the current statistics on application activity.
- Configure the application. Most tabs in the window are identical to similar ones in the policy configuration window (see details in section 15.1.2, page 130). The section further will only describe the functionality different from the features provided for in policies.

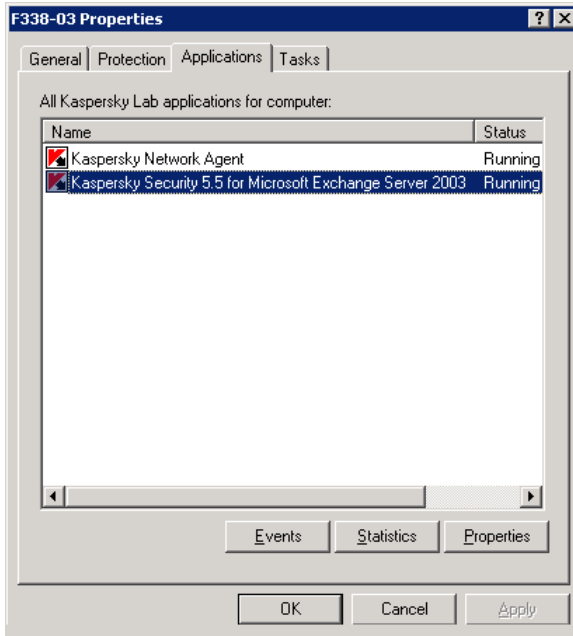


Figure 65. Client computer properties dialog.  
The **Applications** tab



While configuring application parameters, you can only redefine the values allowed for modification in the corresponding group policy.

## 15.2.1. Reviewing the information about application

The **General** tab (see Figure 66) displays general information about Kaspersky Security 5.5 for Microsoft Exchange Server 2003.

The upper window part contains the title of the installed application, its version number, installation date, status (running or stopped on the local computer) and the information about the anti-virus database status.

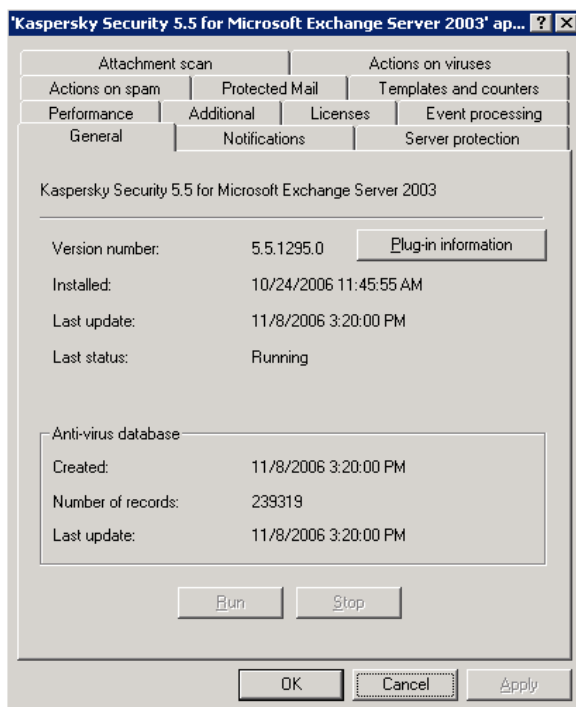


Figure 66. The application properties window.  
The **General** tab

## 15.2.2. Reviewing the license key information

The **Licenses** tab (see Figure 67) is purely informational. It displays the information about the current and the backup license keys installed on the selected computer.

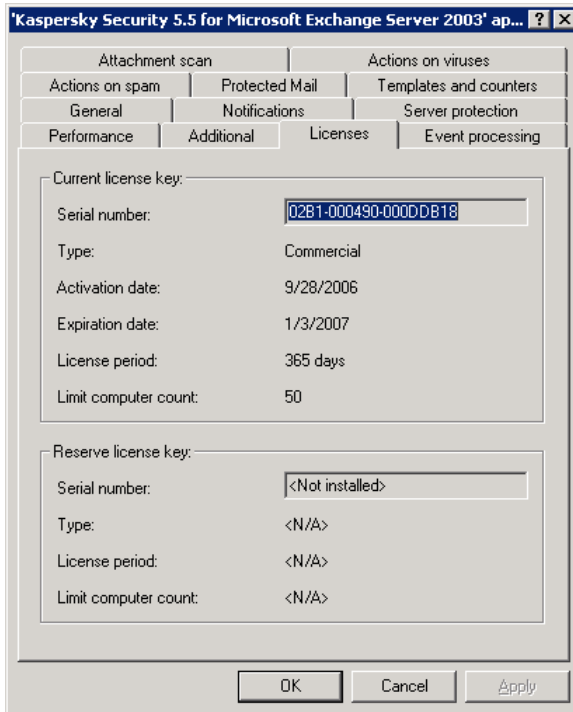


Figure 67. The **Licenses** tab

## 15.2.3. Start background scan

Background scans of e-mail saved on the server and in public folders are run on the **Server protection** tab (see Figure 68).

To start the scan, check **Enable background scan** and assign the scan settings in the window that opens when you click the **Configure** button. To start background scanning immediately, click the **Scan now** button.

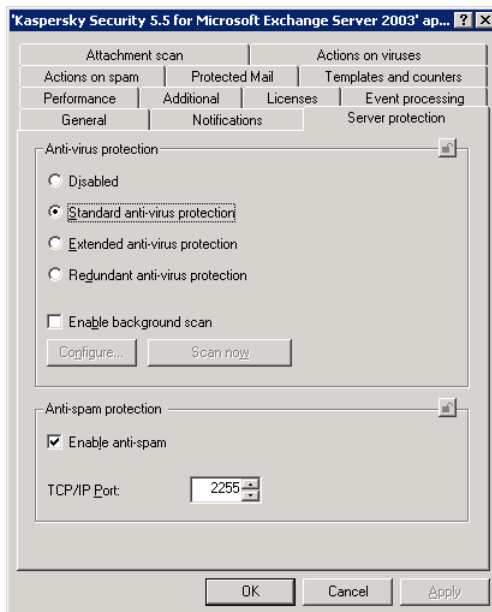


Figure 68. The **Server protection** tab

## 15.2.4. Selection of protected storage

You can use the **Protected Mail** tab (see Figure 69) to enable/disable scanning of mail traffic routed via an Exchange server and also enable/disable protection of mailbox storages or public folders.

By default, the application protects all mailbox storages and public folders existing on the protected mail server. If the number of protected mailboxes exceeds the number indicated in the license, you will have to purchase an additional license or exclude some mailbox storages from the protected area (see details in section 14.5, page 122).

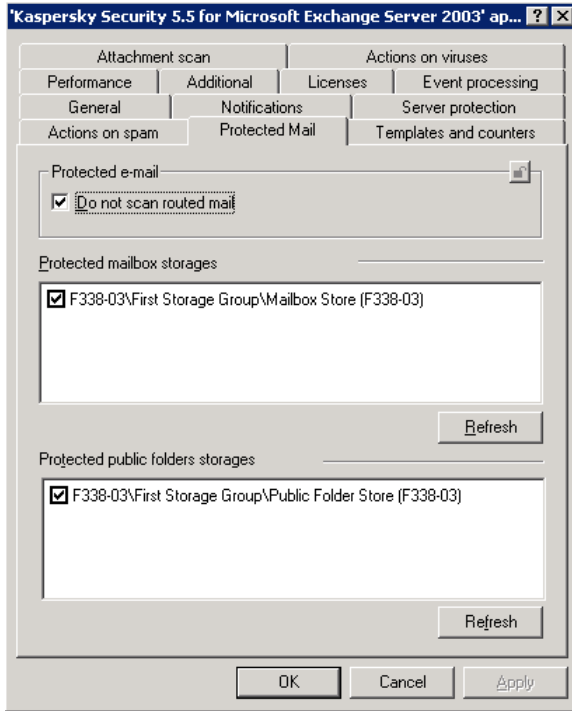


Figure 69. The **Protected Mail** tab

## 15.2.5. Viewing reports

On the **Templates and counters** tab (see Figure 70) you can create report templates, edit their settings, and view generated reports stored on a remote computer.

The procedure for creating a report template is the same as the one described in section 12.1.1, page 104.

To review a report, select the template used to create the report in the **Report templates** list and select the **View reports** command from the right-click menu.

In the **View reports** window (see Figure 71) that opens, select the necessary report and click the **View** button. Doing so will launch the default system browser. Its main window will contain a report on the results of server scanning for the presence of viruses or spam (depending on the report type).

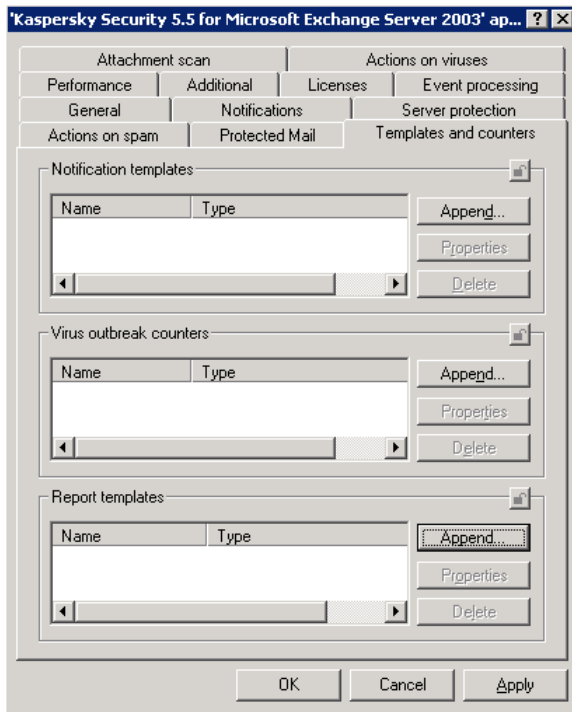


Figure 70. The **Templates and counters** tab

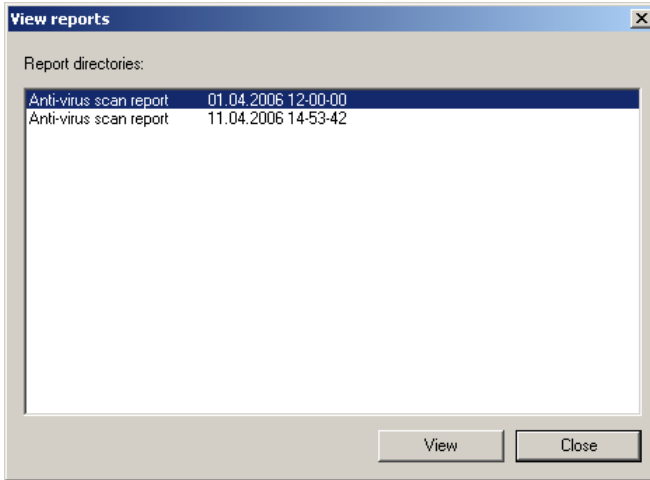


Figure 71. Report viewing window

## 15.3. Task management

During application setup a list of system tasks is generated for each server. The list (see Figure 72) includes the tasks for updating of the anti-virus and content filtration databases.



There is always just a single instance of system tasks on every server. You can run these tasks, configure their settings and schedule; they cannot be deleted.

In addition, you can create license key installation tasks when you need to extend the license to use Kaspersky Security. Tasks of such type can be created not for the local computer only, but also for client groups or a set of computers from different groups (for more on creation and operation of local, group, and global tasks, see the Kaspersky Administration Kit Administrator's Handbook).



*In order to view and manage server tasks:*

1. In the **Groups** folder of the console tree, select the folder containing the required client computer.
2. In the results pane, select a computer with Exchange Server installed and use the **Properties** command from the right-click menu or a similar item from the **Action** menu. Doing so will open a

<Computer name> **Properties** dialog (see Figure 65) in the main program window.



To configure the application tasks on the local computer, select the **Local computer** object (see Figure 47) in the console tree and use the **Properties** command from the right-click menu.

3. Open the **Tasks** tab (see Figure 72). It contains a complete list of tasks existing on that server.

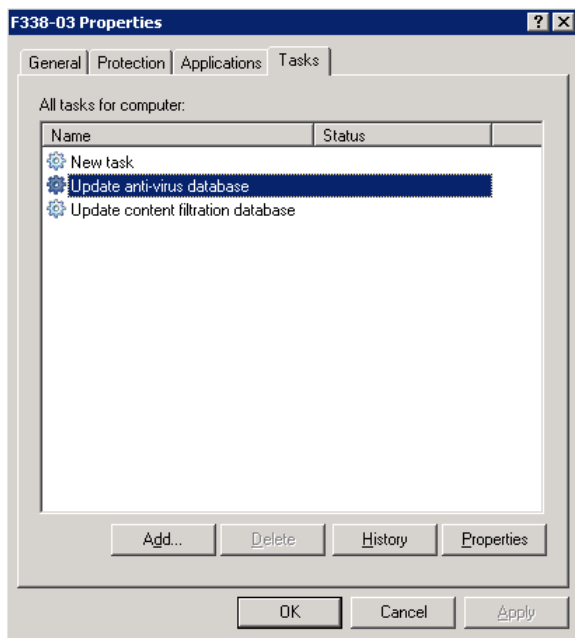


Figure 72. Properties reviewing window for a client computer.  
The **Tasks** tab

The lower window portion contains task management buttons. Click the **Add...** button to create a new task (please refer to the administrator's guide for Kaspersky Administration Kit for details on creating tasks). Click the **Delete** button to remove a task.



Please note, that creation and removal are only available for license key installation tasks. System tasks allow modification of their parameters only.

Click the **Properties** button to review or edit task settings. Doing so will open a <Task name> **task properties** dialog (see Figure 73) where you can:

- Review general information about the task, launch or stop it (the **General** tab).
- Customize specific parameters used to run the task (the **Settings** tab).
- Create its schedule (the **Schedule** tab).
- Configure task launch using an authorized account (the **Account** tab), please refer to the administrator's guide for Kaspersky Administration Kit for details.
- Customize notification settings for the results of task performance (the **Notification** tab). Please refer to the administrator's guide for Kaspersky Administration Kit for details.

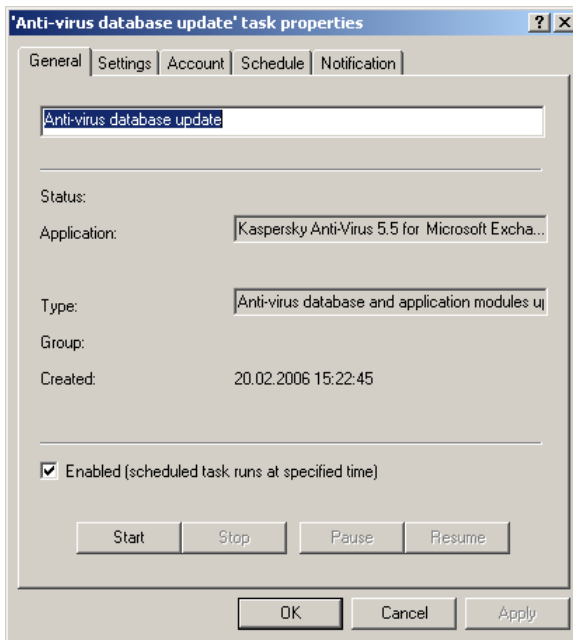


Figure 73. Task configuration. The **General** tab

## 15.3.1. Running and stopping tasks



A task will only be launched on a computer if the corresponding application is running. While the application is stopped, performance of the running tasks will be suspended.

Tasks are launched in accordance with their established schedule. You can temporarily remove certain tasks from the list of scheduled ones. Doing so will not delete the tasks; instead, they will just be skipped.

In addition, you can control tasks manually in the task list window (see Figure 72) and in the dialog for reviewing task settings (see Figure 73).

You can launch a task or resume it using the **Run/Stop** commands of the right-click menu or their counterparts in the **Action** menu.



*In order to run / stop a task manually,*

Select the necessary task in the list (see Figure 72), open the right-click menu and select the **Run/Stop** command or use identical items of the **Action** menu.

You can also initiate such operations from the **General** tab of the task properties window (see Figure 73) using similar buttons.

## 15.3.2. Configuring task parameters

You can configure task parameters in the **Settings** tab of the **<Task name> task properties** (see Figure 73) window. Every task type has its specific settings:

### THE ANTI-VIRUS DATABASE UPDATE TASK

For an anti-virus database update task you can specify the source of updates, settings for running the task under a different user account, and the source used for updating. Available options include the updates' servers of Kaspersky Lab, an HTTP or FTP server or a network directory (see details in section 5.3, page 41).

### THE CONTENT FILTRATION DATABASE UPDATE TASK

For a content filtration database update task you will also have to specify the source of updates. By default, the application will use the same source, which it employs to retrieve updates to its anti-virus database. If you need to set up updating from another source, disable the **Use the parameters of the anti-virus database update task** checkbox.

### THE LICENSE KEY INSTALLATION TASK

The settings window of the license key installation task contains information about the license being added. If you wish to change the key file, click the **Browse** button and use the standard file selection dialog to specify the path to the license key file.

---

# CHAPTER 16. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to questions most frequently asked by users regarding the installation, setup, and operation of Kaspersky Security for Microsoft Exchange Server 2003. We will try to answer them here in detail.



*Question: Can the application be used with other vendors' anti-virus software?*

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 is an anti-virus e-mail application designed to be used in corporate networks. Therefore, it can be used together with Kaspersky Lab's anti-virus applications included into Business Optimal and Corporate Suite software packages (for example, Kaspersky Anti-Virus 5.0 for Windows Workstations, Kaspersky Anti-Virus 5.0 for Windows File Servers), deployed in the network.

In order to avoid conflicts we recommend that you remove any third-party anti-virus software before you install Kaspersky Security 5.5 for Microsoft Exchange Server 2003.



*Question: Why does the application cause a certain decrease in my computer performance and impose a considerable load on the processor?*

The process of virus detection is a purely computational (mathematical) task that involves analysis of structures, checksum calculation and mathematical data transformation. Therefore, the main resource consumed by the anti-virus application is the processor time. Moreover, each new virus added into the anti-virus database adds to the overall scanning time. This is the price that computer users pay for the security of their data.

Unlike other anti-virus software vendors that speed up the scan process by excluding from their databases viruses that are less easily detectable or less frequent in the geographic location of the anti-virus vendor and file formats that require complicated analysis (e.g. PDF files), Kaspersky Lab believes that the purpose of an anti-virus application is to deliver to its users a genuine anti-virus security.

Kaspersky Security allows experienced users to accelerate the anti-virus scanning process to the detriment of the overall security by disabling

scanning of various file types. However, do not forget that this leads to lowering the security level of your computer.



**Question:** *Why do I need a license key? Will my Kaspersky Security application work without it?*

Kaspersky Security 5.5 for Microsoft Exchange Server 2003 will not work without a license key.

If you are still undecided whether or not to purchase a licensed copy of the application, 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 Security license expires?*

After the expiration of the license, Kaspersky Security 5.5 for Microsoft Exchange Server 2003 will continue operating, but databases updating feature will be disabled. Kaspersky Security will continue performing anti-virus and background storage scan as well as the anti-spam scan of incoming e-mail messages, but it will be using obsolete anti-virus and content filtration databases.

When this happens, contact the dealer you purchased your copy of Kaspersky Security application from or Kaspersky Lab Ltd. directly.



**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 an anti-virus application 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.

The number of messages containing SPAM has increased recently. These messages fill up the user's mailbox with useless messages and consume valuable business time. Besides, the mass mailing technologies can be used for propagation of virus outbreaks. Updating our content filtration databases on a regular basis is necessary in order to ensure protection against unwanted e-mail messages.

Kaspersky Lab shortens the update interval for the anti-virus and the content filtration 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 application modules to repair detected vulnerabilities or offer new functionality.



**Question:** *Can an intruder replace my anti-virus database?*

All anti-virus and content filtration databases are supplied with a unique signature verified by the application when it tries to use them. If the signature does not match with the signature assigned by Kaspersky Lab or it is stamped by a later date compared to your license expiry date, the application will not use this database.



**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 this case, the network settings should be configured in the update service settings.

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

The 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.



**Question:** *Sometimes e-mail files in msg format attached to a message become corrupted while being sent so that they cannot be opened. Does it happen because of their scanning by Kaspersky Security?*

The situation has been reproduced during application testing. It has been established that, irrespectively of the presence or absence of installed

Kaspersky Security, files in that format can be damaged during their delivery via an Exchange server.



*Question: After installation of Kaspersky Security on one of servers in our organization, the nearest relay server began generating a queue of messages, which cannot arrive at our server. What should be done in such case?*

The situation results from the application of the **Reject** action to one of the messages containing signs of spam and addressed to your server.

The problem will be resolved without additional actions when the relay server's timeout expires, then receipt of the queued messages will be resumed. You can also delete the rejected message manually from queue and use force connection method for the remaining messages to resolve the issue.

---

# Appendix A. Table of substitution macros

This section lists all the macros used in configuring alternate templates for anti-virus processing of files (see section 6.5, page 57) and settings for virus outbreak counters (see section 11.1, page 95) and notifications (see section 10.1, page 87).

The macros available may differ in each specific case. To add a macro, use the **Macros** button when configuring the corresponding settings.

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 outbreak notifications used only for the <b>One and the same virus detected several times</b> 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

<b>Macros</b>	<b>Macros meaning</b>
<b>%CONTENT_TYPE%</b>	MIME object information
<b>%DATABASE_NAME%</b>	the name of the Microsoft Exchange Server database where the object was detected
<b>%FROM%</b>	displayed sender's name
<b>%MAILBOX_NAME%</b>	name of the mailbox in which the object was detected
<b>%MESSAGE_URL_NAME%</b>	full name of the message where the object was detected
<b>%OBJECT_NAME%</b>	attachment name, not defined for OLE objects and for messages
<b>%OBJECT_TYPE%</b>	object type: message, file, OLE object
<b>%RECV_TIME%</b>	time the message was received
<b>%SCANNER_VERSION%</b>	application version number
<b>%SCANNER_VENDOR%</b>	application vendor name - Kaspersky Lab
<b>%SENT_REPRESENTING_NAME%</b>	displayed name for the message exchange user, provided by the sender
<b>%SERVER_NAME%</b>	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).
<b>%SUBJECT%</b>	message subject

<b>Macros</b>	<b>Macros meaning</b>
<b>%SUBMIT_TIME%</b>	time the message was sent
<b>%TO%</b>	list of message recipients
<b>%PRODUCT_NAME%</b>	application name – Kaspersky Security
<b>%PROCESSED_TIME%</b>	time the file was processed (local time of the server)

---

## Appendix B. Contacting the technical support service

If you encounter problems while using Kaspersky Security, first check if the solution to your problem can be found in this documentation, specifically in the **Frequently Asked Questions** section (see Chapter 16, page 156), or in the **Services/Knowledge base (FAQ)** section of the Kaspersky Lab website ([www.kaspersky.com](http://www.kaspersky.com)).

If you cannot find the solution to your problem in the documentation and the Knowledge Base on the website, please contact Kaspersky Lab Technical Support.

To solve urgent problems, call Technical Support. The numbers are listed in the **Contact Us** section of this documentation (see section D.2, page 179). Users have 24/7 access to phone Technical Support in English, French, German, and Russian. Note that to receive assistance you must be a registered user and must provide a Technical Support specialist with your registration number (if you purchased a boxed version of the program) or information about your order (if you purchased the program through the Internet).

In addition, you can send a query to Technical Support by completing a special form on the Kaspersky Lab website under **Services/Technical Support/Send request to Kaspersky Lab support team**.

When completing the web form, be sure to leave exact information about the Kaspersky Lab product you use and registration data. Try to describe your problem in the greatest detail possible. In the mandatory fields, specify:

- Request type. Select the category that your request belongs to.
- The name of the Kaspersky Lab product that you use (for example, **Kaspersky Security for Microsoft Exchange Server 2003**).
- Text of the request. Describe the problem you encountered while using your Kaspersky Lab product.
- Registration information. Specify your registration type (**license key** if you bought the program in a box, or **online order** if you bought in over the Internet). Depending on the type of registration chosen, enter the serial number of the license or the Internet order number in the field below.

You can view information on your Kaspersky Security 5.5 for Microsoft Exchange Server 2003 serial number on the **License Keys** tab (see Figure 46).

- The e-mail address where the Technical Support team can contact you.

In the next window of the web form, specify your contact information. Enter the security code from automatic registration and click the **Send request** button. The Technical Support team will analyze your problem and will assist you as soon as possible.

---

## Appendix C. 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 Security) 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 the application but not activated yet. 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**.

**Content filtration database** – database, created by Kaspersky Lab's specialists, containing samples of SPAM messages and words and phrases characteristic of SPAM and used for the linguistic analysis of the message content and attachments. Kaspersky Lab is constantly updating this database. Therefore, the administrator must update the database, used by the application, on a regular basis.

**D**

**Deleting 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 (if this option is not disabled, see section 6.5, page 57). You can use this copy later to restore the original object.

**Deleting message** – a method of processing the message containing spam attributes that involves its physical removal from the computer. We recommend using this method for processing messages that definitely contain SPAM. Before the message is deleted, its copy is saved to the backup storage (if this option is not disabled, see section 7.2, page 67).

**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 (if this option is not disabled, see section 6.5, page 57). 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.

**FI**

**Formal messages** – messages automatically generated and sent by mailing programs, mail robots (for example, notifications of undeliverable messages or confirmation of the user's registration at some internet website).

**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 updates servers** – a list of http- and ftp sites of Kaspersky Lab from which the application downloads the anti-virus and the content filtration databases and application modules updates.

**L**

**License key** – a file with \*.key extension that is your personal key required to use the Kaspersky Security application. 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. The application WILL NOT WORK without a license key!

**License period** – a period of time when you are granted the right to use all features of the application. 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 Security for Microsoft Exchange Server 2003. 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.

**Message rejection** – a method of processing the message containing spam attributes that involves blocking the message delivery to the recipient by the Exchange Server. This method is recommended for messages that contain obscene language. Before the message is rejected, its copy is saved to the backup storage (if this option is not disabled, see section 7.2, page 67).

**N**

**Notification template** – a template used to create notifications about infected objects and spam containing messages detected during the 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.

**O**

**Obscene messages** – messages that contain obscene language.

**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 and the anti-spam 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 it with a specified name. The restored file will have the same format as it had before it was first processed by the application.

**S**

**Security Server** – a server component of the Kaspersky Security for Microsoft Exchange Server 2003. Security Server provides the anti-virus protection of the server, protection against SPAM and updating of the anti-virus and the content filtration databases as well as 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**.

**SPAM** – unauthorized mass-mailings of e-mail messages, mostly of advertising nature.

**Storage scan** – see **Background scan**.

**Suspicious object** – an object that contains modified code of a known virus or code that resembles code of a virus, but is not yet known to Kaspersky Lab 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* contains no information about. As a rule, the application detects unknown viruses contained in objects using *heuristic code analyzer* and such objects are assigned the *suspicious* status.

**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 D. Kaspersky Lab

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

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

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

## D.1. Other Kaspersky Lab Products

### Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal has been designed to provide anti-virus protection to personal computers running Microsoft Windows 98/ME or Microsoft Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, Internet, floppy disks, CD, etc. The unique system of heuristic data analysis allows efficient neutralization of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scanning and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had already been scanned during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This feature **considerably increases the speed of the program's operation**.

The application creates a reliable barrier against viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocols and provides highly efficient detection of viruses in mail databases.

The application supports over 700 formats of archived and compressed files and provides automatic scanning of their content as well as removal of malicious code from **ZIP, CAB, RAR, ARJ, LHA** and **ICE** archives.

Configuring the application is made simple and intuitive due to the possibility to select one of three preset protection levels: **Maximum Protection, Recommended** or **High Speed**.

The anti-virus database is updated every hour and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the Internet or the connection has to be changed.

### Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Microsoft Windows 98/ME, Microsoft Windows 2000/NT, Microsoft Windows XP as well as MS Office applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic

retrieval of daily updates for the anti-virus database and the program modules. A unique second-generation heuristic analyzer efficiently detects unknown viruses. A simple and convenient interface allows users to configure the program quickly making work with it easier than ever.

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

- **On-demand scan** of local disks.
- **Real-time automatic protection** of all accessed files from viruses.
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases.
- **Behavior blocker** that provides maximum protection of MS Office applications against viruses.
- **Archive scanning** – Kaspersky Anti-Virus recognizes over 900 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP, CAB, RAR, ARJ, LHA** and **ICE** archives.

### **Kaspersky® Anti-Hacker**

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

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

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

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

## **Kaspersky® Personal Security Suite**

Kaspersky® Personal Security Suite is a software suite designed for organizing comprehensive protection of personal computers running Microsoft Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection of data saved on your computer
- protection against spam for users of Microsoft Office Outlook and Microsoft Outlook Express
- protection of your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

## **Kaspersky Lab News Agent**

The News Agent is intended for timely delivery of news published by Kaspersky Lab, for notifications about the current status of virus activity and fresh news. The program reads the list of available news channels and their content from news server of Kaspersky Lab with specified frequency.

The product performs the following functions:

- It visualizes in the system tray the current status of virus activity.
- The product allows the users to subscribe and unsubscribe from news channels.
- It retrieves news from each subscribed channel with the specified frequency and notifies about fresh news.
- It allows reviewing news on the subscribed channels.
- It allows reviewing the list of channels and their status.
- It allows opening pages with news details in your browser.

News Agent is a stand-alone Microsoft Windows application, which can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

## **Kaspersky® OnLine Scanner**

The program is a free service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. Thus, users can quickly test their computers in case of a slightest suspicion of malicious infection. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

### **Kaspersky® OnLine Scanner Pro**

The program is a subscription service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your computer and disinfection of dangerous files. Kaspersky OnLine Scanner Pro runs directly from your browser. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

### **Kaspersky Anti-Virus® 6.0**

Kaspersky Anti-Virus 6.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, directories or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- **Control of changes within file system.** The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitoring of processes in random-access memory.** Kaspersky Anti-Virus 6.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in standard processes occur.

- **Monitoring of changes in OS registry** due to internal system registry control.
- **Blocking of dangerous VBA macros** in Microsoft Office documents.
- **System restoration** after malicious spyware influence accomplished due to recording of all changes in the registry and computer file system and an opportunity to perform their roll-back at user's discretion.

### **Kaspersky® Internet Security 6.0**

Kaspersky® Internet Security 6.0 is an integrated solution for protection of personal computers against the main information-related threats, i.e. viruses, hackers, spam and spyware. A common user interface allows configuration and management of all solution components.

The anti-virus protection feature includes:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used. The program includes plug-ins for popular e-mail clients (Microsoft Office Outlook, Microsoft Outlook Express and The Bat!) and supports disinfection of their e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- **File system protection:** anti-virus scanning of individual files, directories or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.
- **Proactive protection:** the program performs constant monitoring of application activity and processes running in random-access memory preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

**Protection against Internet-fraud** is guaranteed owing to the ability to recognize phishing attacks, which helps prevent confidential data leaks (first of all, your passwords, bank account and credit card numbers), and block execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The feature **blocking charged phone calls** helps identify software that attempts to use your modem for hidden unauthorized connection to paid phone services and prevents such activity.

Kaspersky® Internet Security 6.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical hacker attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth mode** (owing to the SmartStealth™ technology) **prevents**

**computer detection from outside.** When you switch into that mode, the system will block all network activity except for a few transactions allowed in user-defined rules.

The program employs complex approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites).
- Inspection of phrases in message body.
- Analysis of message text using a self-learning algorithm.
- Recognition of spam sent in image files.

### **Kaspersky® Security for PDA**

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of hand-held computers and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both in internal memory of PDA and smartphones or on memory cards of any type) on user demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

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

### **Kaspersky Anti-Virus Mobile**

Kaspersky® Anti-Virus Mobile provides antivirus protection for mobile devices running Symbian OS and Microsoft Windows Mobile. The program provides comprehensive virus scanning, including:

- **On-demand scans** of the mobile device's onboard memory, memory cards, an individual folder, or a specific file. If an infected file is detected, it is moved to Quarantine or deleted.
- **Real-time scanning** – all incoming and outgoing files are automatically scanned, as will as files when attempts are made to access them
- **Scheduled scans** of data stored in the mobile device's memory
- **Protection from text message spam**

## **Kaspersky Anti-Virus® Business Optimal**

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

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus protection<sup>2</sup> for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux.
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and Linux; *Samba* file storage
- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix , exim, sendmail, and qmail mail systems
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition

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

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

## **Kaspersky® Corporate Suite**

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, Linux; *Samba file storage*

---

<sup>2</sup> Depending on the type of distribution kit.

- *E-mail systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, sendmail, postfix, exim, and qmail mail systems
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition, Microsoft ISA Server 2004 Enterprise Edition
- *Hand-held computers* (PDAs), running Symbian OS, Microsoft Windows CE and Palm OS, and also smartphones running Microsoft Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

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

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

### **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

### **Kaspersky Security® for Microsoft Exchange 2003**

Kaspersky Security for Microsoft Exchange performs anti-virus processing of incoming and outgoing mail messages as well as messages stored at the server, including letters in public folders and filters out unsolicited correspondence using "smart" spam recognition techniques in combination with Microsoft technologies. The application scans all messages arriving at an Exchange Server via SMTP protocol checking them for the presence of viruses using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes. It filters out spam based on formal attributes (mail address, IP address, letter size, heading) and analyzes the content of messages and of their attachments using "smart" technologies, including unique graphic signatures for identifying graphic SPAM. The application scans both the message body and the attached files.

## Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of e-mail stream. The application contains a number of advanced tools for filtering e-mail traffic by name and MIME attachments and a series of tools that reduce the load on the mail system and prevent hacker attacks.

## Kaspersky Anti-Virus® for Proxy Servers

Kaspersky Anti-Virus® for Proxy Server is an antivirus solution for protecting web traffic transferred over HTTP protocol through a proxy server. The application scans Internet traffic in real time, protects against malware penetrating your system while web surfing, and scans files downloaded from the Internet.

## Kaspersky Anti-Virus® for MIMESweeper for SMTP

Kaspersky Anti-Virus® for MIMESweeper for SMTP provides high-speed antivirus scans of SMTP traffic on servers running Clearswift MIMESweeper.

The program is designed as a plug-in for Clearswift MIMESweeper for SMTP and scans for viruses and processes incoming and outgoing e-mails in real time.

## D.2. Contact Us

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

Technical support	Please find the technical support information at <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a> Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">www.kaspersky.com/helpdesk.html</a>
General information	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-mail: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>

---

# Appendix E. 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

ENT. 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](http://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).